Cyberagentur Kritik Realtalk: Was wirklich dahintersteckt

Category: Opinion
geschrieben von Tobias Hager | 3. Februar 2026

Cyberagentur Kritik Realtalk: Was wirklich dahintersteckt

Du willst wissen, warum die Cyberagentur eigentlich so viel heißer Dampf und so wenig Substanz produziert? Willkommen zum Realtalk: Hier gibt’s keine PR-Filter, keine weichgespülten Buzzwords und garantiert keine Hofberichterstattung – sondern eine kritische, tieftechnische Analyse, warum Deutschlands Vorzeigeprojekt in Sachen Cybersicherheit für die einen Hoffnungsträger und für die anderen ein Paradebeispiel für digitale Selbstüberschätzung ist.

- Was ist die Cyberagentur wirklich – und was behauptet sie zu sein?

- Die größten Kritikpunkte: von Intransparenz bis Steuerverschwendung
- Technische Bewertung: Welche Projekte liefern, welche sind reiner Marketing-Sprech?
- Warum Cybersicherheit in Deutschland immer noch im Mittelalter steckt
- Die Rolle von Politik, Lobbyismus und Behörden-Denke im digitalen Wildwuchs
- Welche Technologien von der Cyberagentur tatsächlich relevant sind – und welche nicht
- Wie andere Länder Cybersicherheit ernsthaft aufziehen – und was wir davon lernen müssten
- Pragmatische Schritte: Was echte Online-Marketer und Techies aus dem Drama lernen können
- Fazit: Warum die Cyberagentur mehr als ein PR-Stunt sein muss, um irgendetwas zu bewirken

Die Cyberagentur taucht in den Medien immer wieder als Hoffnungsträger für deutsche Cybersicherheit auf. Doch hinter der schicken Fassade von Innovation und Fortschritt brodelt es gewaltig. Während auf Konferenzen das große Wort geführt wird, herrscht in den Rechenzentren und Amtsstuben oft Stillstand. Wer in der Szene unterwegs ist, weiß: Viele Projekte der Cyberagentur sind wenig mehr als Proof-of-Concepts, die im echten digitalen Alltag untergehen. Zeit, mit Mythen und Missverständnissen aufzuräumen – und endlich darüber zu reden, was wirklich läuft (und was nicht). Hier kommt der knallharte Tech-Check, ohne Rücksicht auf politische Eitelkeiten oder Behördenbefindlichkeiten.

Die Cyberagentur: Anspruch, Realität und der Unterschied dazwischen

Die Cyberagentur wurde 2020 vom Bundesministerium der Verteidigung und dem Bundesinnenministerium ins Leben gerufen. Ziel: Deutschland soll in Sachen Cybersicherheit nicht weiter hinter den USA, Israel oder China herdümpeln, sondern endlich selbst zum Taktgeber werden. Große Worte, große Ambitionen, noch größere Budgets. Im Raum stehen Versprechen von Disruption, bahnbrechenden Innovationen, mehr digitaler Souveränität und dem Schutz kritischer Infrastrukturen. Klingt gut – ist aber nur die halbe Wahrheit.

Schaut man hinter die Kulissen, offenbart sich ein Bild, das weniger von technischer Exzellenz als von politischer Selbstinszenierung geprägt ist. Die Projektpipeline der Cyberagentur liest sich wie das Wunschkonzert einer Abteilung für digitale Transformation: von Quantenkryptografie über Secure Clouds bis hin zu Zero-Trust-Architekturen. Doch wie viel davon ist real, wie viel davon ist bloßes PowerPoint-Bullshit-Bingo?

Genau hier setzt die Kritik an: Während die Cyberagentur nach außen Innovationsführer mimt, sieht die Realität häufig nach Proof-of-Concepts aus, die entweder im Sande verlaufen oder von der Industrie längst überholt

wurden. Der Abstand zwischen Anspruch („Wir revolutionieren Deutschlands Cyberabwehr“) und Wirklichkeit („Wir evaluieren einen Prototyp für verschlüsselte Behördenmails“) ist gewaltig. Wer ein bisschen Code lesen kann und sich in der Tech-Szene auskennt, erkennt schnell: Vieles ist Show, wenig ist Substanz.

Das eigentliche Problem: Die Cyberagentur versteht sich als Thinktank und Innovationsmotor – operiert aber mit den Prozessen und Denkmustern einer klassischen Bundesbehörde. Innovationszyklen, wie sie in Tech-Startups normal sind, werden durch langwierige Ausschreibungen, Vergabeverfahren und politisch motivierte Prioritäten ausgebremst. Das Ergebnis: Die digitale Realität läuft der Cyberagentur regelmäßig davon.

Die größten Kritikpunkte: Von Steuerverschwendung bis IT-Scheininnovationen

Kaum ein Projekt im deutschen Cyberraum steht so sehr im Kreuzfeuer wie die Cyberagentur. Und das aus gutem Grund: Wer sich als digitaler Innovationsmotor inszeniert, muss sich an seinen eigenen Ansprüchen messen lassen. Schauen wir also auf die wichtigsten Kritikpunkte – und warum sie mehr als berechtigt sind.

Erstens: Intransparenz. Die Cyberagentur kommuniziert nach außen mit viel PR, aber wenig echten Details. Welche Projekte wirklich laufen, welche Budgets wie verwendet werden und welche Partner tatsächlich liefern – das bleibt oft im Dunkeln. Für eine Organisation, die sich mit öffentlichen Geldern finanziert, ein Unding. Transparenz ist nicht nur ein nettes Add-on, sondern Grundlage für Vertrauen und Kontrolle.

Zweitens: Steuerverschwendung. Millionenbeträge fließen in Projekte, deren Ergebnisse meist nicht über das Stadium von Konzeptstudien hinauskommen. Das klassische Behördenproblem: Lieber neue Initiativen starten und sich feiern lassen, als alte kritisch evaluieren und Fehler eingestehen. Die Folge: Ressourcen werden gebunden, ohne dass messbare Fortschritte erzielt werden. Wer sich die Summen für externe Beratungen, Studien und Workshops anschaut, kann sich des Eindrucks nicht erwehren, dass hier Geld verbrannt wird, um PowerPoint-Slides zu produzieren.

Drittens: Scheininnovationen. Viele Vorhaben der Cyberagentur klingen auf dem Papier visionär – sind im internationalen Vergleich aber alter Wein in neuen Schläuchen. Quantenkryptografie? Wird in Israel und China längst produktiv getestet. Sichere Cloud-Infrastrukturen? In den USA seit Jahren Standard. Zero-Trust-Architekturen? Für viele Private-Sector-Unternehmen seit 2017 alter Hut. Die Cyberagentur ist häufig eher Nachzügler als Pionier – verkauft aber Kopien aus dem Silicon Valley als eigene Innovation.

Viertens: Fachkräftemangel und Behörden-Denke. Die Cyberagentur hat massive

Probleme, echte IT-Expertise zu gewinnen. Wer für einen Bruchteil des Gehalts beim Staat arbeiten soll, während Amazon, Google und Co. die besten Leute abwerben, entscheidet sich selten für die Bundesbehörde. Ergebnis: Wenige Top-Leute, viel Mittelmaß, und jede Menge „Digitalisierungsmanager“, die noch nie ein produktives System betreut haben.

Technische Bewertung: Was liefert, was ist heiße Luft?

Kommen wir zum Kern der Sache: Welche technischen Projekte der Cyberagentur sind tatsächlich relevant – und welche sind reiner Marketing-Sprech? Wer einmal tiefer in die veröffentlichten Berichte und Projektbeschreibungen schaut, merkt schnell: Die wirklich disruptiven Technologien finden woanders statt. Hier die wichtigsten Beispiele im Überblick:

- Quantenkryptografie: Klingt futuristisch, ist aber in Deutschland bestenfalls Proof-of-Concept. Die echten Fortschritte machen andere Länder – und Unternehmen wie IBM, Google oder chinesische Staatskonzerne. Die Cyberagentur bleibt Zaungast.
- Sichere Cloud-Infrastrukturen: Viel Gerede, wenig produktive Umsetzung. Während der Public Sector in den USA längst auf Zero-Trust und Multi-Cloud setzt, werden hierzulande noch Grundsatzdiskussionen geführt.
- Zero-Trust-Architekturen: Theoretisch spannend, praktisch kaum umgesetzt. Die meisten Behördennetze sind noch nicht einmal auf Segmentierung oder restriktive Zugriffskonzepte umgestellt.
- KI-basierte Bedrohungsanalyse: Hier gibt es tatsächlich spannende Ansätze, aber die Projekte stecken meist in der Pilotphase. Von echter Operationalisierung keine Spur.
- Supply-Chain-Security: Ein Hype-Thema, aber die Cyberagentur bleibt hinter den Möglichkeiten zurück. Während die Industrie längst auf automatisiertes Monitoring und Continuous Security setzt, wird hier noch Papier geprüft.

Was fehlt: Open-Source-Engagement, echte Produktentwicklung, rapid Prototyping, DevSecOps – kurz: alles, was moderne Tech-Unternehmen ausmacht. Stattdessen dominieren Projekte, die sich im Klein-Klein von Studien, Workshops und Konsortien verlieren. Wer die echten Herausforderungen der Cybersicherheit lösen will, muss Code shippen, nicht nur Konzepte schreiben.

Die technische Realität: Die Cyberagentur ist zu langsam, zu bürokratisch, und zu sehr auf politische Effekte bedacht. Der technologische Output bleibt überschaubar. Die Projekte, die tatsächlich Relevanz hätten, werden durch Prozesse, Gremien und Abstimmungen zerredet. Innovation by Committee – und das funktioniert im Tech-Bereich selten bis nie.

Cybersicherheit made in Germany: Warum wir international hinterherhinken

Deutschland ist in Sachen Cybersicherheit längst nicht mehr auf Augenhöhe mit den internationalen Big Playern. Während in den USA und Israel Cyberabwehr als nationales Topthema mit massiver Unterstützung und radikalem Innovationsgeist vorangetrieben wird, herrscht hierzulande Behörden- und Lobbyismus-Mikado. Die Cyberagentur ist ein Paradebeispiel für dieses Dilemma: Viel Anspruch, wenig Output, noch weniger Geschwindigkeit.

Woran liegt’s? Zum einen an der politischen Struktur: Während in Staaten wie Israel militärische und zivile Cyberabwehr Hand in Hand arbeiten und gemeinsam mit Startups und Industrie echte Produkte entwickeln, blockieren in Deutschland Kompetenzgerangel, Datenschutzängste und Amtsstubenlogik jede Form von Agilität. Der Föderalismus tut sein Übriges: Wer für was zuständig ist, weiß oft niemand so genau. Das Ergebnis: Kein klarer Fokus, kein Tempo, keine echten Durchbrüche.

Zum anderen fehlt es an Risikobereitschaft und Experimentierfreude. Während andere Nationen Fehler als notwendige Lernschritte begreifen, herrscht hierzulande die Angst vor dem Scheitern. Innovationskultur? Fehlanzeige. Die Cyberagentur ist in ihrer DNA eine Behörde – und das merkt man an jeder Ecke. Wer disruptive Technologien will, muss bereit sein, auch mal auf die Nase zu fallen. In Deutschland wird lieber alles bis zur Unkenntlichkeit abgesichert, bevor überhaupt irgendwas live geht.

Und schließlich: Fachkräftemangel. Die Cyberagentur ist nicht in der Lage, mit Tech-Giganten um die besten Leute zu konkurrieren. Wer echte Talente will, muss sie auch entsprechend bezahlen und ihnen Entscheidungsfreiheit geben. Doch genau daran hapert es. Der deutsche Beamtenapparat ist das Gegenteil von attraktiv für Hacker, Entwickler und Security-Architekten, die wirklich etwas bewegen wollen.

Was echte Marketer und Techies aus dem Cyberagentur-Drama lernen können

Was bleibt von der deutschen Cyberagentur außer Schlagzeilen? Für alle, die wirklich im digitalen Raum arbeiten – ob als Marketer, Entwickler, CTO oder Admin – liefert das Drama immerhin einige wertvolle Lektionen. Wer digital erfolgreich sein will, muss sich auf eines verlassen: Selbst machen, statt auf Behörden warten.

- Setze auf Open Source, wo immer es möglich ist – und baue eigene Security-Kompetenz auf, statt dich auf politische Versprechen zu verlassen.
- Teste neue Technologien pragmatisch aus, statt auf die perfekte Lösung zu warten. In der Zeit, in der Behörden noch Workshops veranstalten, sind andere schon live.
- Automatisiere alles, was automatisiert werden kann – von Patch-Management bis Incident-Response. Die Cyberagentur zeigt, wie gefährlich es ist, wenn technische Prozesse manuell ablaufen.
- Baue echte Partnerschaften mit Tech-Unternehmen, Startups und Communities auf. Innovation entsteht im Netzwerk, nicht im Behördenbüro.
- Setze auf kontinuierliches Monitoring, Penetration-Tests und Red Teaming – nicht auf einmalige Zertifizierungen und Audits.

Wer auf den digitalen Staat wartet, wartet für immer. Die Cyberagentur kann bestenfalls Impulse geben – aber die eigentliche Arbeit passiert in den Unternehmen, bei den Techies und Marketers, die nicht auf politische Vorgaben, sondern auf funktionierende Systeme setzen. Wer wirklich sicher sein will, muss selbst denken, selbst machen, selbst patchen. Punkt.

Fazit: Cyberagentur Kritik – Mehr als ein PR-Stunt?

Die Cyberagentur ist ein Symbol für Deutschlands digitalen Spagat: Zwischen Innovationsanspruch und Behördenrealität, zwischen Budget und Output, zwischen Pressemitteilung und technischer Substanz. Wer sich von den Hochglanz-Präsentationen blenden lässt, verpasst die eigentliche Lektion: Cybersicherheit entsteht nicht durch Meetings und PowerPoints, sondern durch echten Code, mutige Entscheidungen und radikale Transparenz.

Wer heute auf die Cyberagentur als Retter hofft, hat die digitale Realität nicht verstanden. Die Zukunft der Sicherheit liegt in agilen Teams, Open Source, technischer Exzellenz und echter Fehlerkultur – nicht in politisch motivierten Labs. Wer im Online-Marketing, in der IT oder im Digital Business unterwegs ist, sollte sich auf eines verlassen: Auf die eigene Kompetenz, nicht auf Behörden. Die Cyberagentur bleibt ein Lehrstück dafür, wie man es nicht machen sollte – und vielleicht, mit ein wenig Glück, irgendwann auch für echten Wandel. Bis dahin: Patch yourself. Trust no one. Und hör auf, auf Wunder aus Berlin zu warten.