Cyberagentur Kritik Standpunkt: Klartext für Entscheider

Category: Opinion
geschrieben von Tobias Hager | 4. Februar 2026

Cyberagentur Kritik Standpunkt: Klartext für Entscheider

Die deutsche Cyberagentur feiert sich als Bollwerk gegen digitale Bedrohungen – doch hinter der hochglanzpolierten PR-Fassade brodelt es gewaltig: ineffiziente Prozesse, fragwürdige Vergabepraxis, Kompetenz-Mimikry und ein Innovationsverständnis aus dem letzten Jahrzehnt. Wer als Entscheider wirklich wissen will, was im deutschen Cyber-Sicherheitszirkus schiefläuft, bekommt hier den ungeschönten, technischen und strategischen Klartext, den die Branche so dringend braucht – und den Politik und Beratungsagenturen nie liefern werden.

- Die Cyberagentur – Anspruch, Realität und die große Lücke dazwischen
- Warum das deutsche Innovationsverständnis im Cyberbereich systematisch versagt
- Kritikpunkte an Strategie, Technik und Management – mit knallharten Beispielen
- Vergabepraxis, Überbürokratisierung und der Mythos vom „digitalen Schutzwall“
- Technische Defizite, die Entscheider kennen müssen, bevor sie Millionen verbrennen
- Gefährliche Abhängigkeiten von US-Tech und das Fehlen echter Souveränität
- Warum KI, Cloud und Zero Trust in deutschen Behörden oft nur Buzzwords sind
- Konkrete Maßnahmen – wie Entscheider aus dem deutschen Cyber-Schlaf erwachen
- Fazit: Wer jetzt nicht disruptiv umdenkt, riskiert die digitale Handlungsunfähigkeit

Cyberagentur – das klingt nach Elite, nach technisch versierten Teams, die Deutschland mit modernsten Technologien gegen die globale Cybermafia verteidigen. Die Wahrheit ist: Die Cyberagentur ist ein Paradebeispiel für das, was im deutschen Innovationssystem falsch läuft. Buzzwords wie „Resilienz“, „KI“ und „Zero Trust“ werden in Pitches und Pressemitteilungen inflationär durchgekaut – doch die technologische Substanz bleibt oft auf dem Niveau von PowerPoint-Folien, die ein Berater in sechs Stunden zusammengekleistert hat. Wer als Entscheider auf solche Narrative hereinfällt, riskiert nicht nur Budget-Fehlallokation, sondern die digitale Zukunftsfähigkeit ganzer Organisationen.

Der folgende Standpunkt ist keine ideologische Polemik, sondern basiert auf tiefgehender technischer Analyse, Erfahrungswerten aus internationalen Cyberprojekten und messerscharfer Kritik an den realen Strukturen der Cyberagentur. Hier gibt es keine weichgespülten PR-Floskeln, sondern detaillierte Einblicke in die technischen und organisatorischen Schwachstellen – und klare Handlungsempfehlungen, wie Entscheider endlich aufwachen und handeln müssen.

Cyberagentur: Anspruch, Realität und die große Innovationslücke

Die Cyberagentur wurde gegründet, um Deutschlands digitale Souveränität zu bewahren und technologische Exzellenz im Cyberraum zu fördern. Das Ziel: disruptive Innovationen für die nationale Sicherheit entwickeln – jenseits von klassischen Beschaffungsprozessen, schnell, agil und visionär. Die Realität? Ein träger Tanker, bei dem Innovationsprojekte in endlosen Gremienrunden, Abstimmungsschleifen und Ausschreibungs-Exzessen versanden.

Der zentrale Webfehler ist systemisch: Statt echten technologischen Durchbruchsprojekten zu fördern, konzentriert sich die Cyberagentur oft auf safe bets – inkrementelle Verbesserungen und Scheininnovationen. Das mag auf dem Papier für politische Entscheider risikolos wirken, verhindert aber, dass Deutschland in entscheidenden Zukunftsfeldern wie KI-Security, Post-Quantum-Cryptography oder automatisierter Threat-Response überhaupt eine relevante Rolle spielt.

Im internationalen Vergleich wirkt das Cyberagentur-Modell wie aus der Zeit gefallen. Während die USA mit DARPA oder Israel mit Unit 8200 strategisch auf radikale Experimente und technologische Eigenständigkeit setzen, bleibt die deutsche Cyberagentur ein Hybrid aus Behörde, Beraterbude und politischem Feigenblatt. Die Folge: Innovationszyklen, die langsamer sind als die durchschnittliche Lebensdauer eines Mainstream-Smartphones.

Für Entscheider bedeutet das: Wer sich auf die Cyberagentur als Innovationsmotor verlässt, setzt auf ein System, das den Status quo zementiert – und zwar mit Ansage. Die Lücke zwischen Anspruch und Realität ist nicht nur peinlich, sondern brandgefährlich.

Kritik an Strategie und Technik: Was wirklich schiefläuft

Die Cyberagentur gibt sich gerne als Think Tank für die digitale Elite. Doch ein Blick hinter die Kulissen offenbart eine technologische Schieflage, die man nur als fahrlässig bezeichnen kann. Das beginnt bei der Auswahl und Förderung von Projekten: Statt disruptive, risikoreiche Technologien zu pushen, finanziert man häufig Lösungen, die seit Jahren am Markt sind – getarnt als „Pilotprojekte“ oder „Leuchttürme“.

Ein Kernproblem: Die technische Due Diligence ist oft mangelhaft. Projekte werden nach politischem Konsens und Präsentationsfähigkeiten bewertet, nicht nach realer technischer Substanz. Kritische Themen wie DevSecOps, Supply Chain Security, Zero Trust Architekturen oder Offensive Security (Red Teaming) werden zwar als Schlagworte verwendet, aber selten in ihrer technischen Tiefe verstanden oder umgesetzt.

Typische technische Defizite, die Entscheider kennen müssen:

- Fehlende Integration von Continuous Security Testing in Entwicklungsprozesse – viele Projekte setzen weiterhin auf manuelle, punktuelle Audits statt automatisierter Penetrationstests und Red Team Simulationen.
- Mangelhafte API-Sicherheit – oft werden Schnittstellen entwickelt, ohne auf Authentifizierung, Rate Limiting oder Input Validation auf Protokollebene zu achten.
- Vernachlässigung von Cloud-Native Security – statt Infrastructure-as-

Code (IaC) und automatisierter Compliance-Checks dominieren On-Premise-Denken und klassische Perimeter-Schutzkonzepte.
- Unzureichende Logging- und Monitoring-Strategien – viele Systeme liefern zwar Daten, aber ohne SIEM-Integration oder automatisierte Alerting-Mechanismen.
- Kaum Verständnis für moderne Angriffsmethoden – viele Entscheider unterschätzen die Geschwindigkeit und Komplexität von Threat Actors, die längst auf KI-gestützte Angriffstools setzen.

Die Cyberagentur produziert so Projekte, die im internationalen Maßstab bereits beim Proof of Concept zum Museumsstück taugen. Für den deutschen Steuerzahler ist das eine teure Technologie-Illusion.

Vergabepraxis, Bürokratie und der Mythos vom digitalen Schutzwall

Ein weiteres Fiasko: Die Vergabepraxis. Wer meint, Innovation und öffentlicher Sektor passen nicht zusammen, findet in der Cyberagentur ein Lehrbuchbeispiel. Ausschreibungen sind so konstruiert, dass nur Großunternehmen oder Netzwerkakteure mit Berater-Gen die Zugangshürde nehmen. Start-ups, disruptive Technologiefirmen oder forschungsstarke KMU? Fehlanzeige.

Die Folge: Projekte werden mit endlosen Compliance-Richtlinien, Datenschutzpapieren und Abstimmungsrunden so lange totoptimiert, bis jede technische Brillanz zum Standardfall degradiert ist. Wer „schnelle Beschaffung“ verspricht, wird von der Realität deutscher E-Vergabe-Tools und Vergabehandbücher brutal eingeholt. Hier regiert der Prozessfetischismus – und nicht der Wille, Cyberrisiken wirklich zu minimieren.

Der Mythos vom digitalen Schutzwall ist dabei gefährlich: Nur weil Millionen in Projekte mit schicken Titeln wie „Cyber Shield“ oder „AI Defense Suite“ fließen, ist kein System sicherer. Entscheider müssen endlich lernen, dass Cybersicherheit nicht mit Budget, sondern mit technischer Exzellenz, Geschwindigkeit und radikaler Fehlerkultur erkauft wird. Alles andere ist Selbstbetrug.

Ein typischer Verlauf deutscher Cyberprojekte:

- Projektantrag mit umfassender Marktanalyse (Copy-Paste aus internationalen Reports)
- Monatelange Gremiensitzungen, in denen der Scope so weichgekocht wird, dass niemand mehr weiß, was das Ziel ist
- Vergabe an einen Konsortialführer, der primär für Projektdokumentation und Management-Meetings sorgt
- Minimaler technischer Output, maximaler Overhead

Das Ergebnis: Ein „digitaler Schutzwall“, der vor allem gegen Innovation schützt – und nicht gegen reale Bedrohungen.

Technische Defizite: Wo Deutschlands Cyberagentur digital abgehängt ist

Wer die technischen Reports der Cyberagentur liest, erkennt schnell: Viele Lösungen basieren auf veralteten Paradigmen. Während internationale Player auf automatisierte Incident Response, KI-gestützte Erkennung von Advanced Persistent Threats (APT) und hardwarebasierte Trusted-Execution-Umgebungen setzen, wird in Deutschland noch über „zentrale Firewalls“ und „VPN-Pflicht“ gestritten. Willkommen in 2010.

Ein weiteres Defizit: Die Abhängigkeit von US-Software und Public-Cloud-Anbietern. Statt eigene Open-Source-Stacks zu fördern oder europäische Technologien zu integrieren, werden Standardlösungen von Microsoft, Amazon oder Palo Alto eingekauft – inklusive aller geopolitischen Risiken und Vendor-Lock-in-Probleme. So entsteht keine Souveränität, sondern eine neue digitale Abhängigkeit.

Besonders kritisch ist das KI-Verständnis: Während international längst KI-basierte Anomalieerkennung und Automated Threat Intelligence in Echtzeit eingesetzt werden, beschränkt sich der deutsche Ansatz oft auf Keyword-Bingo in Management-Präsentationen. Die reale technische Umsetzung bleibt weit hinter dem Stand der Technik zurück. Gleiches gilt für Zero Trust – ein Begriff, der inflationär verwendet wird, aber in der Praxis meist auf „Zwei-Faktor-Authentifizierung und VPN“ reduziert wird. Die Architektur echter Zero Trust Environments erfordert granulare Mikrosegmentierung, Continuous Authentication und Identity Federation auf Protokollebene – davon ist die Cyberagentur meilenweit entfernt.

Ein weiteres Beispiel: Cloud Security. Während internationale Standards wie CIS Benchmarks, Cloud Security Posture Management (CSPM), Infrastructure as Code Scanning und Policy-as-Code längst Praxis sind, wird in deutschen Projekten häufig noch per Hand konfiguriert – mit fatalen Folgen für Skalierbarkeit und Sicherheit.

Konkrete Maßnahmen: Was Entscheider jetzt tun müssen

Die gute Nachricht: Es gibt einen Weg aus dem deutschen Cyber-Dornröschenschlaf. Aber er ist unbequem, disruptiv und verlangt technisches Verständnis auf Entscheider-Ebene. Wer weiterhin auf Berater-PowerPoints und bunte Innovationsgrafiken setzt, wird langfristig abgehängt. Hier die

wichtigsten Schritte, um als Entscheider wirklich Wirkung zu erzielen:

1. Technisches Know-how aufbauen
   Als Entscheider reicht es nicht, Buzzwords zu verstehen. Setze auf regelmäßige Deep Dives in Themen wie DevSecOps, Cloud Security, KI-Security und Incident Response. Lass dich nicht von PR-Folien blenden, sondern fordere technische Proofs und Live-Demos ein.
2. Projektförderung radikal neu denken
   Fördere disruptive, risikoreiche Ansätze. Belohne Fehlerkultur und Rapid Prototyping. Setze auf technische Exzellenz statt auf „safe bets“ mit maximaler Dokumentation.
3. Vendor-Lock-in verhindern
   Setze auf Open Source, offene Standards und API-first-Ansätze. Vermeide Abhängigkeiten von US-Riesen, indem du europäische und unabhängige Alternativen priorisierst.
4. Automatisierung und Continuous Security einfordern
   Verlange, dass alle Projekte automatisierte Security-Tests, Infrastructure as Code und Monitoring by Default implementieren. Keine Ausnahme, keine Ausreden.
5. Multi-Cloud und Zero Trust wirklich leben
   Zero Trust ist mehr als ein Passwortmanager und ein VPN. Setze auf echte Mikrosegmentierung, kontinuierliche Identitätsprüfung und feingranulare Policy-Engines. Multi-Cloud-Strategien reduzieren die Abhängigkeit und erhöhen die Resilienz.
6. Agile Beschaffung durchsetzen
   Lass Vergabekriterien von Technikern prüfen, nicht von Verwaltungsexperten. Fördere Start-ups und kleine, hochspezialisierte Anbieter. Beschleunige den Innovationszyklus durch Rapid Prototyping und agile Sprint-Vergaben.

Fazit: Disruptive Ehrlichkeit statt digitaler Selbsttäuschung

Die Cyberagentur ist ein Symptom – nicht die Ursache – für das tief sitzende technologische und strategische Problem der deutschen Cyber-Sicherheitsarchitektur. Wer als Entscheider weiter auf PR-getriebene Innovation und Berater-Narrative setzt, verschläft nicht nur die nächste Technologiewelle, sondern riskiert die digitale Handlungsunfähigkeit ganzer Organisationen. Es geht nicht um mehr Budget, sondern um mehr technische Exzellenz, Geschwindigkeit und den Mut, echte Risiken einzugehen.

Wer jetzt nicht radikal umdenkt, wird vom internationalen Wettbewerb gnadenlos abgehängt. Der Standpunkt ist klar: Nur wer als Entscheider technologische Tiefe fordert, Innovationszyklen radikal beschleunigt und Abhängigkeiten minimiert, kann in der digitalen Welt bestehen. Alles andere ist digitales Placebo – und das können wir uns längst nicht mehr leisten.