MICROSENS

Anmerkungen zur nationalen Rechenzentrumsstrategie aus Sicht eines mittelständischen deutschen Herstellers

MICROSENS GmbH & Co. KG
Küferstraße 16
59067 Hamm

Hannes Bauer, Dipl.-Ing.
Technischer Leiter und Gründer
hbauer@microsens.de

Frank Konrad, Dipl.-Ing.
Geschäftsführer
fkonrad@microsens.de

Das Unternehmen

Die Fa. MICROSENS GmbH & Co. KG ist ein mittelständisches Unternehmen mit Sitz in Hamm/NRW.
Zu den Schwerpunkten des Unternehmens gehören die Entwicklung, Fertigung und Vermarktung von aktiven Netzwerk-Komponenten (Switches, Glasfaser-Multiplexer) mit eigener Entwicklung von Hardware und Software und Fertigung am Standort.
Aufgrund der aktuellen Marktentwicklung, vor allem getrieben durch den rapiden Auf- und Ausbau von KI Kapazitäten, liegt ein starker Fokus unserer Unternehmenstrategie für die nächsten Jahre auf dem Markt für Rechenzentrumsvernetzung.

Aktuelle Herausforderungen

Aktuell sehen wir uns als deutscher Hersteller mit folgenden Herausforderungen konfrontiert:

Dominanz globaler Wettbewerber
Große internationale Konzerne (Cisco, Huawei, Arista, Juniper) dominieren den Markt. Sie verfügen über hohe F&E-Budgets und setzen Standards, wodurch deutsche Anbieter, insbesondere im KMU-Bereich, im globalen Vergleich nur schwer mithalten können.

Abhängigkeit von Halbleitern und Spezialkomponenten
Gleichzeitig stammen Schlüsselkomponenten wie ASICs oder optische Komponenten überwiegend aus den USA oder Asien. Fehlende europäische Alternativen führen zu Abhängigkeiten und Preisrisiken. Auch der technologische Zugang zu solchen Herstellern ist aufgrund der geringeren wirtschaftlichen Relevanz für KMUs beschränkt.

Zunehmende Virtualisierung und Software-Defined Networking (SDN)
Kunden fordern softwaregesteuerte Netzwerke mit Automatisierung und offenen APIs. Hersteller müssen ihre Hardware mit leistungsfähigen Software-Stacks kombinieren. Die Anpassung von OpenSouce-Stacks auf standardisiere Hardware steht bei uns im Fokus, um die hohen Anforderungen an Sicherheit und Compliance erfüllen zu können.

Security- und Compliance-Druck
Neue regulatorische Vorgaben wie Cyber Resilience Act (CRA) und NIS2 erfordern Funktionen wie Secure Boot, Hardware-Root-of-Trust, durchgängige Verschlüsselung und SBOMs. Der Entwicklungsaufwand steigt dadurch erheblich und erfordert spezialisierte Entwickler, die aufgrund des Fachkräftemangels im High-Tech-Bereich nur schwer verfügbar sind.

Vor dieser Situation stehen wir

Der explosionsartig steigende Einsatz von KI im allen Bereichen der Wirtschaft und des täglichen Lebens hat große Auswirkungen auf die zukünftige wirtschaftliche Leistungs- und Wettbewerbsfähigkeit der deutschen Wirtschaft. Die Souveränität unseres Landes kann nur sichergestellt werden, wenn wir in der Lage sind, die eingesetzten Technologien nicht nur zu kontrollieren, sondern sie zu beherrschen und weiter zu entwickeln. Je größer der technologische Vorsprung anderer Nationen, konkret der USA und China, auf diesem Gebiet ist, desto schwieriger wird es werden, nationale Interessen noch durchzusetzen und damit die eigene Zukunft aktiv gestalten zu können.

Das tun wir

Die größten Sicherheitsrisiken gehen heutzutage nicht von der Hardware, sondern primär von der Software aus, die die Funktion der Hardware steuert. Daher arbeiten wir mit internationalen Partnern zusammen, um standardisierte Hardware als Plattform für unsere eigene Software zu nutzen. Damit ist es möglich, weiterhin die Kostenvorteile des Weltmarkts zu nutzen und dennoch maximale Kontrolle über die Funktionalität zu haben und Cyber-Sicherheit zu garantieren.

Das benötigen wir

Eine nationale Rechenzentrumsstrategie muss Souveränität, Sicherheit und Innovation gleichwertig berücksichtigen. Als deutscher Netzwerktechnik-Hersteller benötigen wir klare Rahmenbedingungen, die:

1. technologische Unabhängigkeit fördern,
2. faire Wettbewerbsbedingungen schaffen,
3. Investitionen ermöglichen,

um Deutschland als führenden Standort für sichere und wettbewerbsfähige Rechenzentren etablieren.

Wie uns der Staat unterstützen kann

Die Rolle des Staates aus Herstellersicht sollte darin liegen, durch Maßnahmen wie die folgenden die richtigen Anreize zu setzen:

1. Verbindliche Berücksichtigung deutscher Hersteller in Bundes- und Landesprojekten. Öffentliche Referenzprojekte (Bundescloud, kommunale Rechenzentren) sollten bevorzugt mit deutscher Technik ausgestattet werden.
2. Förderprogramme für Entwicklung, Test und lokale Fertigung von Netzwerktechnik.
3. Steuerliche Anreize für Unternehmen, die Netzwerktechnik in Deutschland entwickeln und produzieren
4. Um schneller und praxisnah Innovationen erproben zu können, empfehlen wir den Aufbau eines deutschen RZ-Testnetzes für Hersteller.
5. Entwicklung praxisnaher Normen (z.B. CRA-Umsetzung) gemeinsam mit Herstellern, um bürokratische Hürden abzubauen und Wettbewerbsnachteile ggü. anderen Märkten und Teilnehmern zu verringern.
6. Investitionssicherheit durch langfristige RZ-Strategie auch über 2030 hinaus.

Fazit

Deutschland steht an einem technologischen Wendepunkt: Ohne eigene starke Hersteller von Netzwerktechnik und eine leistungsfähige Rechenzentrumsinfrastruktur droht eine wachsende Abhängigkeit von internationalen Anbietern.
Eine nationale Rechenzentrumsstrategie muss daher klare industriepolitische Rahmenbedingungen setzen. Nur so können deutsche Hersteller und Betreiber die Wettbewerbsfähigkeit sichern und Deutschland langfristig als führenden Standort für hochperformante und resiliente Rechenzentren etablieren.

Hamm, 2025-09-19