Dr. Ferri Abolhassan

# »Sicherheit ist kein Kostenblock, sondern eine Wachstumsversicherung«

Die zunehmende Bedrohungslage im Cyberraum zwingt Unternehmen und Behörden zu einem radikalen Umdenken beim Schutz kritischer Infrastrukturen. Dr. Ferri Abolhassan, CEO von T-Systems und Mitglied des Telekom-Vorstands, treibt den Aufbau souveräner digitaler Infrastrukturen voran und sieht Sicherheit als essenziellen Wachstumsmotor für den deutschen Mittelstand und Großunternehmen. Im Interview spricht er über digitale Resilienz und erläutert, wie Europa eigene technologische Standards setzen kann.

Interview **Ayman Duran** Bild **zVg**

**Dr. Abolhassan, wie hat sich Ihre Rolle vom »Security-Macher« bei der Telekom hin zum Gestalter von digitaler Souveränität und Resilienz für Wirtschaft und Staat entwickelt?**
Beide Themen begleiten mich schon meine ganze Karriere. Als ich vor zehn Jahren die IT-Division von T-Systems geleitet habe, habe ich die heutige »T-Sec« mit aufgebaut. Jetzt, als CEO von T-Systems und Mitglied des Telekom-Vorstands, verstehe ich mich mehr als Architekt von souveränen digitalen Infrastrukturen. Unsere Aufgabe als gesamtes Team Magenta ist es, eine digitale Grundversorgung zu schaffen, vergleichbar mit Strom oder Wasser – eben nur für Daten, KI oder Cloud-Lösungen. Damit stärken wir konkret die Resilienz und Wettbewerbsfähigkeit von Unternehmen, Behörden und damit auch die des Landes.

**Warum ist digitale Resilienz heute genauso systemrelevant wie klassische physische Sicherheit?**
Digitale Resilienz bedeutet, Systeme so zu bauen, dass sie gegen Cyberangriffe, Sabotage und Ausfälle gerüstet sind. Wie in der physischen Sicherheit muss man dafür sorgen, dass man bei Attacken handlungsfähig bleibt. Wenn wir kritische Störungen in Fabriken, Krankenhäusern oder bei Energieversorgern haben – man denke an den Stromausfall in Berlin im Winter durch einen Brandanschlag –, dann kann das Millionen und viel an Vertrauen kosten und im schlimmsten Fall Menschenleben gefährden. Wir erleben eine digitale Zeitenwende, in der Sicherheit und Verfügbarkeit genauso mitgedacht werden müssen wie Funktionalität und Kosten.

**Sie gelten als Mann für Vertrieb und Wachstum. Wie verkaufen Sie das oft als Kostenfaktor betrachtete Thema »Cybersecurity« an Vorstände?**
Es ist ein Denkfehler, den Unternehmen heute nicht mehr machen sollten. Sicherheit ist kein Kostenblock, sondern eine Wachstumsversicherung. Vorstände unterschreiben heute nicht mehr nur für Umsatz und Marge, sondern auch für Resilienz, Lieferfähigkeit und Compliance – auch gegenüber den Kunden und der Legislation. Ich argumentiere nicht in Firewalls, sondern in Geschäftsrisiken: Können sie jederzeit produzieren? Können sie jederzeit für ihre Kundschaft oder Patient:innen da sein? In meinen Gesprächen mit CEOs und CIOs sehe ich vermehrt, dass die wachsende Bedrohungslage erkannt und ernst genommen wird.

**Ist absolute Sicherheit heute eine Illusion und müssen wir uns stattdessen primär auf schnelle Wiederherstellung und Resilienz konzentrieren?**
Absolute Sicherheit ist im digitalen Raum leider eine Illusion. Wer anderes behauptet, verspricht zu viel. Man kann sich bestmöglich schützen, aber nie zu 100 Prozent. Es geht eher darum, Sicherheitsvorfälle schnell zu erkennen, einzudämmen und IT-Systeme wieder sicher hochzufahren. Dies erfordert umfassende Resilienz – vom Design der Architektur über Notfallpläne bis hin zu Zero-Outage-Standards.

> **Wir erleben eine digitale Zeitenwende, in der Sicherheit und Verfügbarkeit genauso mitgedacht werden müssen wie Funktionalität und Kosten.**
>
> – Dr. Ferri Abolhassan

**Sie haben vor über zehn Jahren »Zero Outage« bei T-Systems angestoßen. Welche Lehren daraus sind für Behörden, Krankenhäuser, Energieversorger und andere Betreiber kritischer Infrastrukturen heute am wichtigsten – auch mit Blick auf NIS-2?**
»Zero Outage« ist seit Jahren unsere DNA. Qualität und Sicherheit sind keine Projekte, sondern eine Denkweise. »Zero Outage« hat gezeigt, dass man Standards, Prozesse und Training konsequent durchhalten muss, um Störungen und Ausfälle niedrig zu halten. Das ist kein Sprint, sondern ein Marathon. Für Energieversorger oder Banken bedeutet das, nicht nur Checklisten abzuarbeiten, sondern Ende-zu-Ende zu denken: Von der Lieferkette über Betriebsprozesse bis hin zu klaren Verantwortlichkeiten im Krisenfall.

**Wie verändern der AI Act und NIS-2 die Spielregeln für Unternehmen und Behörden – und was müssen Entscheider:innen jetzt tun, um nicht nur compliant, sondern wirklich widerstandsfähig zu werden?**
Beide werden oft als Bürokratiemonster bezeichnet. Das sehe ich anders. Sie sind ein guter Sicherheitsgurt für die digitale Transformation, weil sie uns zwingen, Risiken ernst zu nehmen, Verantwortlichkeiten zu klären und Resilienz messbar zu machen. Wer das proaktiv nutzt und vertrauenswürdige digitale Dienste aufbaut, hat im Markt einen echten Vorteil. Unsere Rolle ist es, diese Regeln in praxistaugliche Lösungen zu übersetzen, damit es für Kunden machbar, einfach und greifbar ist.

**Viele sprechen von »digitaler Souveränität«. Was macht eine KI- oder Cloud-Lösung aus Ihrer Sicht wirklich souverän – technisch, rechtlich und politisch?**
Es gibt drei Dimensionen: Datensouveränität heißt, dass die Daten in einem europäischen Rechenzentrum liegen, verschlüsselt sind und die Kundschaft die Kontrolle hat. Rechtliche Souveränität stellt sicher, dass kein Zugriff durch ausländische Behörden möglich ist. Technologisch fragen wir: Haben wir offene Standards, Interoperabilität und die Fähigkeit, Workloads zu verlagern, statt in einem proprietären Lock-in zu landen? Erst wenn Unternehmen genau die souveräne Cloud-Lösung erhalten, die zu ihren Anforderungen passt, entsteht echte digitale Freiheit.

**Haben wir in Europa den Kampf um Hardware und Plattformen verloren und können wir unsere Souveränität nur noch auf der Software- und Sicherheitsebene verteidigen?**
Im Wettlauf um die großen Hyperscaler-Plattformen und Teile der Hardwareproduktion sind andere vorne. Aber Souveränität heißt nicht, alles selbst zu bauen, sondern strategische Stellhebel zu kontrollieren: Daten, Prozesse, Standards und Sicherheit. In München beispielsweise haben wir am 4. Februar gemeinsam mit Nvidia, SAP, Siemens und anderen die weltweit erste industrielle KI-Cloud eröffnet. Das ist ein Beispiel dafür, wie wir mitspielen können: durch Partnerschaften und Allianzen. Es ist noch viel zu tun. Aber natürlich müssen wir auch damit klarkommen, dass wir in gewissen Feldern abhängig sind.

**Die Telekom engagiert sich jetzt stärker im Defense-Bereich, unter anderem über ein Millioneninvestment in Quantum Systems, ein Drohnen-Start-up aus München. Was war der Hintergrund und inwiefern profitiert die Gesellschaft von dieser Kooperation?**
Ohne Sicherheit gibt es keine Freiheit. Das gilt in der digitalen wie in der physischen Welt. Mit unserem Engagement im Defense-Bereich antworten wir auf die Bedrohungslagen aus dem Aus- und Inland. Das lässt sich auch auf den Verteidigungssektor, Spionageabwehr, Schutz von Stadien beispielsweise bei Großereignissen wie EM oder WM und insgesamt auf den Bevölkerungsschutz übertragen. Es geht dabei um aktiven Schutz unserer Netze, demokratischen Institutionen und letztlich der Menschen. Und das halten wir für eine notwendige Sache.

**Öffentliche Sicherheit ist mehr als Technik: Was müssen Staat, Wirtschaft und Wissenschaft jetzt konkret unternehmen, damit Europa bei KI, Cloud und Defense nicht nur aufholt, sondern eigene Standards setzt?**
Wir dürfen nicht naiv sein. Man könnte sagen: Der Zug ist abgefahren. Ich sage: Der Zug ist nur so lange abgefahren, wie es keinen neuen Zug gibt. Und wir setzen gerade in München einen neuen aufs Gleis. Das ist unser Beitrag für die Unternehmensinitiative »Made for Germany«. Wir wollen hier vorangehen, Deutschland und Europa besser und stärker machen.