

Branchen-Anwendung

Digitale Souveränität: Die Grundlage moderner Wehrhaftigkeit

Die sicherheitspolitische Zeitenwende ist da. Konflikte werden nicht mehr nur mit Panzern und Raketen entschieden, sondern auch im digitalen Raum, während gleichzeitig das Vertrauen in globale Partnerschaften erodiert. Die Kontrolle über sensible Daten ist somit zur entscheidenden Ressource für die Handlungs- und Verteidigungsfähigkeit Deutschlands und Europas geworden. Doch sie ist an zwei Fronten bedroht.

Die doppelte Herausforderung: Angriff auf die äußere und innere Sicherheit

Äußere Sicherheit: Die digitale Frontlinie

Die Zusammenarbeit mit Bündnispartnern und der Schutz der eigenen Rüstungsindustrie sind entscheidend. Doch genau hier bestehen fatale Sicherheitslücken wie:

- **Verbesserungswürdige Interoperabilität:** Im NATO-Strang können alle miteinander kommunizieren. Der Austausch zwischen nationalen Einheiten und Kommandobehörden ist dagegen noch nicht standardisiert. Die Folge sind riskante Medienbrüche und Drehstuhlschnittstellen.
- **Spionage in der Lieferkette:** Wirtschaftskriminalität gegen Zulieferer – oft durch staatliche Akteure – gefährdet die Einsatzbereitschaft der Streitkräfte und die Sicherheit der Soldaten.

Innere Sicherheit: Der administrative Kollaps

Die staatliche Handlungsfähigkeit hängt von der sicheren digitalen Zusammenarbeit der Sicherheitsbehörden ab – ein Anspruch, der in der Praxis immer wieder an Systemgrenzen scheitert und beispielsweise zu folgenden Risiken führt:

- **Gestörter Informationsaustausch:** Ein Angriff auf den Datenaustausch zwischen Behörden – sei es durch Manipulation von Inhalten oder gezielte zeitliche Verzögerung der Kommunikation – kann die nationale Gefahrenabwehr substanziell schwächen.
- **Verletzung der Vertraulichkeit:** Gelangen vertrauliche Daten in die falschen Hände, kann dies die Arbeit der Sicherheitsbehörden massiv beeinträchtigen.

idgard: Souveränität durch technische Garantien

idgard ist eine hochsichere Plattform für Datenaustausch und Kollaboration, entwickelt und betrieben in Deutschland. Die patentierte Sealed-Cloud-Technologie ersetzt vertragliche Hoffnung durch physikalische Fakten und garantiert den Schutz der Daten im gesamten Lebenszyklus: Während der Übertragung (data in transit), im Speicher (data at rest) und – entscheidend – auch während der Verarbeitung (data in use).

Unbefugte können zu keinem Zeitpunkt auf unverschlüsselte Inhalte zugreifen. Das gilt sowohl für idgard als Betreiber als auch für Administratoren, sofern sie keine explizite Freigabe durch den Datenbesitzer erhalten haben. Das Need-to-know-Prinzip wird zur physikalischen Tatsache.

Absolute Vertraulichkeit

- **Zero-Knowledge-Prinzip:** Macht Spionage durch Anbieter oder Dritte technisch unmöglich und schützt vor Zugriffen durch ausländische Behörden.
- **Schutz vor operativer Aufklärung:** Die Verschlüsselung von Metadaten verhindert die Analyse von Befehls- und Kommunikationsketten.

Einsatzfähigkeit & Rechtssicherheit

- **Flexibler Einsatz:** Als hochsicherer Cloud-Service oder gehärtete, mobile Appliance für den autarken Betrieb in Gefechtsständen und Krisengebieten.
- **Automatischer Selbstschutz:** Sofortige Löschung aller aktiven Daten im RAM bei physischem Fremdzugriff auf die gehärtete Appliance. Die verschlüsselte Version auf der Festplatte bleibt bestehen.
- **Garantierte Sicherheit:** Als Lösung „Made in Germany“ unterliegt idgard deutschem Recht. Die Sicherheit ist by Design in der Architektur verankert und durch Zertifikate (z. B. ISO 27001) belegt.

Nahtlose Kollaboration

- **Volle Datenhoheit:** Sicherer, klassifizierter Austausch mit Partnern (wie NATO, EU, Industrie) durch granulare Zugriffskontrolle, ohne die Souveränität zu verlieren.
- **Hohe Nutzerakzeptanz:** Sofort einsetzbar durch Integration in gewohnte Umgebungen (Netzlaufwerk, Office-Add-Ins).

Ihre nächsten Schritte zu digitaler Souveränität

Die Stärkung der digitalen Wehrhaftigkeit ist eine der zentralen strategischen Aufgaben unserer Zeit. idgard ist die praxiserprobte Lösung für alle Ebenen – von der Zusammenarbeit im Ministerium bis zum Datenaustausch im Einsatz – und zugleich ein Baustein für eine Software Defined Defense. Der Lösung vertrauen bereits über 200.000 Anwender aus dem öffentlichen Sektor, der Hochsicherheitsindustrie und anderen kritischen Infrastrukturen.

„Unser Ziel ist es, Deutschland und Europa bis 2028 so aufzustellen, dass es koordinierten Cyberattacken standhält.“

Arved Graf von Stackelberg, CEO idgard und DriveLock

Beginnen Sie jetzt. Sprechen Sie mit unseren Experten über Ihre spezifischen Anforderungen und sichern Sie die Handlungsfähigkeit Ihrer Organisation.

Mehr zu den Lösungen von idgard erfahren Sie unter www.idgard.com oder kontaktieren Sie uns unter sales@idgard.com für ein persönliches Gespräch.