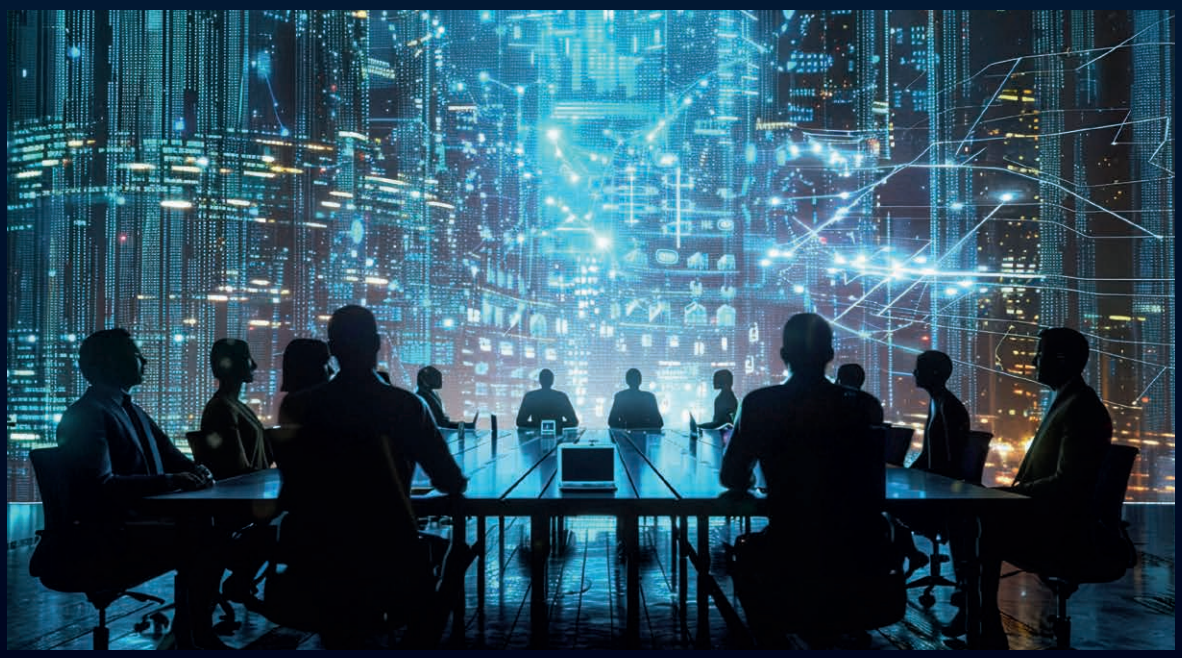
NATIONAL SECURE CLOUD

NSC und VS-Arbeitsplatz – Ihr Duo für höchste Sicherheit

Entwicklung einer souveränen und sicheren Cloud in Deutschland von führenden Cybersecurity-Experten

IABG | infodas | KERNKONZEPT | utimaco® | XELERA

Inhaltsverzeichnis



IABG – Wir gestalten Sicherheit

Seit mehr als sechs Jahrzehnten übernimmt die IABG Verantwortung für die Sicherheit von Staat und Gesellschaft. Das klare Ziel: Stets einen Schritt voraus zu sein und die Zukunft schon heute zu denken. Dies gilt auch für die digitale Souveränität Deutschlands. Daher haben wir zusammen mit weiteren deutschen Unternehmen das Programm National Secure Cloud (NSC) aufgesetzt.

Die IABG ist ein führendes europäisches Technologie-Unternehmen, das unabhängige und produktneutrale Beratung für den Einsatz sicherheitsrelevanter Systeme bietet. Wir verantworten als Koordinatorin des NSC-Programms dessen strategische Steuerung und Weiterentwicklung. Dazu gehören die Erfüllung höchster Sicherheitsanforderungen von Bedarfsträgern wie Behörden und Militär sowie die Gewährleistung einer entsprechend sicheren und souveränen digitalen Infrastruktur einschließlich der Interoperabilität mit internationalen Standards.

Innerhalb des NSC-Konsortiums definiert die IABG die Gesamtarchitektur aus Hardware und Software und sorgt für das sichere Management von Lösungen für Platform-as-a-Service (PaaS), und Software-as-a-Service (SaaS) inklusive konsequenter Integration von Open Source Software.

Industrieanlagen-Betriebsgesellschaft mbH
Einsteinstraße 20
85521 Ottobrunn

Patrick Rund
Senior Manager
Digitale Transformation
rund@iabg.de
+49 89 6088 3713
www.iabg.de

Höchste Sicherheit ohne Kompromisse

Die kritische IT-Infrastruktur in Behörden und militärischen Einrichtungen erfordert höchste Sicherheitsstandards. Gerade in Zeiten verstärkter Cyberattacken und einer zunehmenden internationalen Vernetzung benötigen die Bedarfsträger sichere Arbeitsumgebungen und Cloud-Lösungen, die strengen Anforderungen an Vertraulichkeit und Datenschutz genügen sowie die digitale Souveränität Deutschlands berücksichtigen. Zentrale Bausteine für eine solche Lösung sind die National Secure Cloud (NSC) und der VS-Arbeitsplatz – beides entwickelt von einem Konsortium vertrauenswürdiger deutscher IT-Unternehmen unter Führung der IABG.

Unsere Lösungen: NSC und VS-Arbeitsplatz

Die NSC ist eine hochsichere Cloud-Infrastruktur, die Daten unterschiedlicher Sicherheitsstufen gleichzeitig verarbeiten kann. Sie erfüllt dabei die strengen Anforderungen der Verschlusssachenanweisung (VSA). Ein zentrales Merkmal der NSC ist die Trennung von Sicherheitsdomänen. Dadurch kann sie mehrere Schutzniveaus auf derselben Hardware betreiben – mit hoher Kosteneffizienz. Die NSC nutzt Open-Source-Technologien, um Transparenz und Nachvollziehbarkeit zu gewährleisten. Diese offene Architektur verringert die Abhängigkeit von den proprietären Technologien internationaler Anbieter – sogenannten Hyperscalern – und ermöglicht zugleich eine einfache Anpassung an spezifische Anforderungen.

Die National Secure Cloud

- Hochsichere Cloud-Infrastruktur gemäß Anforderungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI).
- Sicherheitsdomänen und sichere Domänenübergänge für Behörden und Militär.
- Hohe Leistungsfähigkeit, Interoperabilität und Skalierbarkeit.

Der VS-Arbeitsplatz ergänzt die NSC durch eine sichere Arbeitsumgebung. Auch hier liegt der Fokus auf Open-Source-Lösungen, die der digitalen Souveränität dienen. Sie sind speziell auf die Bedürfnisse von Organisationen mit hohen Sicherheitsanforderungen zugeschnitten. Mechanismen wie Zugriffskontrollen und Verschlüsselung sorgen für die Vertraulichkeit und Integrität von Daten. Zudem gibt es einen Schutz vor Schadsoftware und unbefugtem Zugriff. Der VS-Arbeitsplatz ist daher für die Bearbeitung von Verschlusssachen bis zur VS-Einstufung GEHEIM ausgelegt.

Der VS-Arbeitsplatz

- → Modulare Lösung aus europäischen Open-Source-Anwendungen.
- → Skalierbar für große Organisationen mit tausenden Nutzern.
- → Bearbeiten von Verschlusssachen bis zur VS-Einstufung GEHEIM.
- → Kompatibel mit ZenDiS openDesk.

Sicherheit und technische Merkmale

Die NSC kombiniert Software, Services und speziell für den Cloud-Use-Case entwickelte Sicherheitshardware. Sie nutzt einen BSI-zugelassenen Hypervisor, der mehrere Sicherheitsdomänen auf einer einzigen Hardware verwaltet. Die strikte Trennung der Domänen sorgt für maximale Sicherheit und erlaubt es, Daten bis zur VS-Einstufung GEHEIM zu verarbeiten. Spezielle Security Gateways ermöglichen den Datenaustausch zwischen unterschiedlichen Sicherheitsdomänen – ebenfalls bis zur VS-Einstufung GEHEIM. Kryptografische Hardware-Sicherheitsmodule sorgen dabei für den Schutz vor unberechtigtem Zugriff.

Die NSC und der VS-Arbeitsplatz erfüllen höchste Sicherheitsstandards und sind trotzdem benutzerfreundlich, skalierbar und kosteneffizient. Sie lassen sich leicht in bestehende Infrastrukturen integrieren. Dies ermöglicht es Bedarfsträgern, ihre vorhandene Software weiter zu nutzen. Die Modularität der Systeme hilft zudem, neue Technologien wie Künstliche Intelligenz (KI) unkompliziert zu integrieren.

Im militärischen Bereich funktionieren die Systeme bei Bedarf autark ohne Netzverbindung, auch auf kleinstem Raum. Sie bieten zudem eine hohe Interoperabilität mit Bündnispartnern, etwa im Rahmen von NATO-Operationen. Die NSC und der VS-Arbeitsplatz sind modulare, hochsichere und flexible Lösungen, die sich an unterschiedliche Anforderungen anpassen lassen. Damit sind sie die idealen Werkzeuge für Behörden, militärische Einrichtungen und andere sicherheitskritische Organisationen in Deutschland.

Im Visier: tägliche Angriffe auf deutsche Regierungsnetze

- Das BSI registriert jeden Tag 250.000 neue Schadprogramm-Varianten.
- Allein die Bundesverwaltung erhält im Schnitt täglich 775 E-Mails mit Schadsoftware.
- Pro Tag sperrt das BSI 370 Websiten für den Zugriff aus den Regierungsnetzen.

Download PDF:
BSI Lagebericht
IT-Sicherheit.

Cyberspionage: Angriffe im diplomatischen Umfeld

- SolarWinds-Supply-Chain-Angriff, der u. a. mehrere US-Regierungsbehörden betraf (2020).
- Angriff auf das zivile Geschäft des Rüstungskonzerns Rheinmetall (2023).
- Russischer Militärgeheimdienst greift SPD-Zentrale und Rüstungsunternehmen an (2024).
- Cyberattacke – vermutlich aus China – auf das britische Verteidigungsministerium (2024).
- IT-Infrastruktur der CDU-Parteizentrale muss nach einem Angriff vom Netz genommen werden (2024).

Allein diese kleine Auswahl an weltweiten Vorfällen aus den vergangenen Jahren verdeutlicht die anhaltende Bedrohung durch Cyberspionage, die auf diplomatische Kommunikation und sensible Informationen abzielt. Häufige Angriffsvektoren sind Phishing, Malware und Kompromittierungen der Lieferkette.

Zwei typische Angriffe auf die IT des öffentlichen Sektors

1. Der IT-Dienstleister der Industrie- und Handelskammern entdeckte am 3. August 2022 auffälliges Verhalten in seinen IT-Systemen und fuhr sie zur Schadensvermeidung herunter. Dadurch wurden alle 79 IHK in Deutschland vom Internet getrennt, was Webseiten offline schaltete und E-Mail-Kommunikation unmöglich machte. Auch interne Anwendungen waren betroffen. Nach intensiver Prüfung startete der Dienstleister die Systeme wieder, doch einzelne Kammern waren auch Monate später noch beeinträchtigt.

2. 2022 und 2023 gab es Ransomware-Angriffe auf 27 kommunale Verwaltungen und Betriebe. Betroffen waren Kommunen unterschiedlicher Größe, von einer kleinen Gemeinde mit 2.800 Einwohnern bis hin zu einer Großstadt mit über 1,8 Millionen Bewohnern. Ziel der Angriffe waren Stadt- und Kreisverwaltungen, Nahverkehrsbetriebe, Energieversorger, Wohnungsbaugesellschaften, Stadtreinigungsbetriebe und ein Schulamt.

Digitale Souveränität mit der National Secure Cloud

Die Entwicklung der National Secure Cloud (NSC) greift die aktuellen Diskussionen um digitale Souveränität und staatliche IT-Sicherheit auf. Insbesondere Behörden und Streitkräfte arbeiten täglich mit Daten gemäß Verschlusssachenanweisung (VSA) und benötigen zudem einen hohen Grad an Souveränität. Die NSC ist eine speziell auf diese „Schutz"-Bedürfnisse zugeschnittene Cloud-Lösung. Aber was macht sie so besonders? Im Interview erläutert Patrick Rund (Senior Manager und Programmleiter Digitale Transformation bei der IABG) die Vorteile der NSC.

Patrick Rund
Senior Manager
Digitale Transformation
IABG

Die Entwicklung einer souveränen und für Verschlusssachen geeigneten Cloud- und Arbeitsplatzlösung ist keine einfache Aufgabe. Welche Idee steckt dahinter?

Unsere zentrale Idee war eine in Deutschland und für Deutschland entwickelte Cloud-Lösung, die zwei Aufgaben erfüllt: erstens die digitale Souveränität zu stärken und zweitens nachweisbar sicherer als gewöhnliche Cloud-Lösungen zu sein.

Die bekannten internationalen Anbieter erfüllen oft nicht die sehr hohen Anforderungen der VSA jenseits von VS-NfD. Das Sicherheitsniveau ist aufgrund der Komplexität und Architektur dieser Lösungen nur bedingt nachweisbar bzw. messbar. Das erschwert die Zulassung/Akkreditierung (beispielsweise durch das BSI) solcher Angebote enorm.

Darum haben wir unsere Komponenten so entwickelt, dass die Nutzer nicht nur die volle Kontrolle über ihre Daten haben, sondern die „Zulassungsfähigkeit", etwa durch das BSI, möglich ist. Gleichzeitig können stets höchste Sicherheitsstandards eingehalten werden. Dabei setzen wir auf Open-Source-Software, eine nachvollziehbare sowie möglichst standardisierte Architektur und eine handhabbare Entwicklungs-Roadmap, um ein hohes und vor allem auch messbares Sicherheitsniveau sowie digitale Souveränität zu garantieren.

Zu den Zielgruppen gehören Behörden, Militärs und andere staatliche Akteure. Vor welchen Herausforderungen stehen diese Zielgruppen bei ihrer Arbeit heute?

Die größte Herausforderung ist der Schutz VS-eingestufter Daten angesichts der zunehmenden Digitalisierung, Kollaboration und Vernetzung, auch in der Kommunikation zwischen Behörden und militärischen Einrichtungen (national und international). Dazu müssen IT-Systeme und neue Technologien mit der VSA in Einklang gebracht werden. Doch ein hundertprozentiger Schutz ist auch hier nahezu unmöglich.

Behörden müssen trotz aller Herausforderungen darauf achten, weiterhin handlungsfähig zu bleiben. Dazu ist es notwendig, die Vorteile neuer Technologien effizient und zügig zu heben, etwa Künstliche Intelligenz oder das Internet der Dinge (IoT). Damit lassen sich die Folgen der demografischen Entwicklung und des dadurch entstehenden Fachkräftemangels zumindest abschwächen. Es gilt, in immer komplizierteren Netzwerken von Geräten stabile und sichere Kommunikationsbeziehungen sowie

Services zu gewährleisten und dabei die wachsende Menge an Daten zu beherrschen.

Dabei sind die Nutzer dieser Lösungen, egal ob in der Administration oder Sachbearbeitung, auf eine unkompliziert zu betreibende und leicht bedienbare Lösung angewiesen. Oftmals sind die eigentlichen Sachthemen bereits komplex genug. Das IT-System bzw. die Applikation darf den Lösungsweg nicht noch komplexer machen.

Die angebotenen Lösungen müssen allerdings bezahlbar bleiben und innerhalb der Rahmenbedingungen staatlicher Etats verwirklicht werden können. Das gilt insbesondere in Zeiten wie diesen mit einem engen Haushaltsplan.

Für all diese Herausforderungen ist das Konzept einer Cloud als IT-System mit ihren eindeutigen Vorteilen eine gute Ausgangsbasis.

Welche unterschiedlichen Anforderungen haben die Zielgruppen?

Öffentliche Verwaltungen und Dienste benötigen im Umgang mit VS-Daten eine sichere und kosteneffiziente Lösung, mit der sie im eigenen Bereich, mit Bürgern sowie mit anderen Behörden interagieren können – sicher, DSGVO- und VSA-konform. Ein Beispiel dafür ist der ressortübergreifende Datenaustausch zwischen Polizei und Justiz. Hinzu kommt, dass einige staatliche Akteure, wie z. B. das Außenministerium, die Funktionen für die Verarbeitung von Verschlusssachen weltweit verfügbar benötigen. Zudem müssen entsprechende IT-Systeme für diese Nutzergruppen räumlich flexibel sein, was der „mobile VS-Arbeitsplatz“ ist.

Im militärischen Bereich sind die Anforderungen an Sicherheit und Vertraulichkeit ebenfalls durchweg sehr hoch. Im Bereich der Funktionalität ist das Militär außerdem mit einer Vielzahl an teilweise proprietären und hardwaregebundenen Waffen- und Führungssystemen besonders komplex. Insbesondere hier muss sukzessive die Trennung von Soft- und Hardware erfolgen und eine weitere Standardisierung, auch im NATO-Rahmen, ist zielführend. Eine wichtige Anforderung ist zudem die Möglichkeit, dass sich die Systeme im Ernstfall schnell verlegen lassen und autark ohne Netzverbindung funktionieren. Die Interoperabilität mit Bündnispartnern, bspw. im Rahmen von sogenannten Multi-Domain-Operations der NATO, ist eine weitere wichtige Anforderung.

Nahezu alle Zielgruppen brauchen natürlich eine platz- und ressourcensparende Lösung. Die Fähigkeit, Daten zwischen IT-Systemen mit unterschiedlicher VS-Einstufung zu verschieben, ist ebenfalls von entscheidender Bedeutung. Genauso wichtig ist eine hohe Flexibilität des Systems. Denn nicht nur im Krisenfall müssen in kürzester Zeit neue Applikationen oder Updates zur Verfügung stehen.

Synopsis: Staatliche Akteure benötigen IT-Systeme, die nutzerfreundlich, flexibel, ressourcensparend, skalierbar, autark betreibbar, interoperabel und mit allen nationalen und internationalen Sicherheitsstandards kompatibel sind. Sicherlich keine leichte Aufgabe, aber genau hier kommen die klassischen Vorteile einer Cloud ins Spiel, sofern die Cloud-Technologien für VS-IT bzw. VSA-konform ertüchtigt werden. Und genau dafür sorgen wir zusammen mit unseren Partnern.

Warum sind NSC und VS-Arbeitsplatz die besten Lösungen? Was können sie, was andere nicht können?

Die National Secure Cloud und der mit ihr perfekt harmonierende VS-Arbeitsplatz haben einige Vorteile gegenüber anderen Lösungen. Zunächst einmal verfolgen wir ein offenes Konzept und alles ist Open-Source basiert. Wenn ein Kunde eine bestimmte Anforderung hat, können wir gemeinsam mit dem BSI relativ unkompliziert eine realistische, den Anforderungen entsprechende und sichere Lösung bieten. Letztlich steckt der Aufbau eines Ökosystems dahinter: andere Hersteller und Anbieter können und sollen ihre Lösungen in das „Gesamtsystem NSC" integrieren. So steigern wir Sicherheit und Souveränität.

Sowohl die NSC als auch der VS-Arbeitsplatz sind von Grund auf für höchste Sicherheitsanforderungen konzipiert. Das lässt sich am besten mit dem Schlagwort „Security by Design" zusammenfassen. Wir sorgen also zunächst für VSA-konforme Sicherheit und dann für das „Look & Feel". So basiert die NSC auf bereits vom BSI zugelassenen Komponenten, die sukzessive weiterentwickelt werden. Wir gehen sozusagen Schritt für Schritt voran und schaffen eine Balance zwischen Performance, Sicherheit und Zulassungsfähigkeit. Die ideale Ausgangslage, um die unterschiedlichen Anwendungsszenarien der Bedarfsträger umzusetzen und eine BSI-Zulassung zu erhalten.

Die National Secure Cloud (NSC) ist gezielt für die VS-IT folgender Bedarfsträger ausgelegt:

- **Regierungen mit hohem IT-Sicherheitsanspruch (inkl. angeschlossener Ministerien und Verwaltungen)**
  Für Regierungen und ihre nachgelagerten Behörden steht digitale bzw. Daten-Souveränität ganz oben auf der Agenda. Zudem ist es für diese Bedarfsträger wichtig, einen Vendor-Lock-in zu vermeiden. Stattdessen sollen klassische Produkte der Hyperscaler durch Open-Source-Anwendungen wie den VS-Arbeitsplatz ersetzt oder ergänzt werden.

- **Bundeswehr und andere militärische Organisationen (z. B. NATO oder befreundete Staaten)**
  Auch im militärischen Kontext ist Datensouveränität sehr wichtig. Zusätzlich müssen hier internationale Standards (z. B. der NATO) berücksichtigt werden. Die technischen Anforderungen sind damit erheblich höher für Regierungen. Der Technologie-Stack der NSC erfüllt all diese Anforderungen. Aktuelle Entwicklungen zeigen, dass die Bundeswehr sich an die ZenDiS-Lösung openDesk anlehnt. Der VS-Arbeitsplatz ist die ideale Ergänzung und voll kompatibel mit openDesk.

- **Regulierte Industrien**
  Regulierte Branchen wie die Pharmaindustrie verwenden erhebliche finanzielle Mittel auf die Entwicklung medizinischer Produkte, die zusätzlich meist einen sehr komplexen und mehrjährigen Zulassungsprozess durchlaufen. Geheimhaltung während des gesamten Prozesses von der Idee bis zur Zulassung ist daher von herausragender Bedeutung, um den Wissensvorsprung sowie den Return on Investment zu sichern.

Vielleicht noch zwei Beispiele aus der Technik: unser Hypervisor kann mehrere Sicherheitsdomänen auf einer Hardware laufen lassen und sorgt somit für Kosten- und Platzeinsparungen. Und durch die Virtualisierung von Sicherheitsfunktionen ermöglichen wir dem Kunden, flexibel auf Anpassungsbedarfe zu reagieren. Denn das Deployment einer Software ist deutlich einfacher als der Umbau von Hardware.

Unser offenes Geheimnis ist also ein Mix aus innovativer Technik, Philosophie und strukturierter Kommunikation mit den entsprechenden Stakeholdern – denn es geht nur zusammen. Wie ich anfangs bereits gesagt habe: es ist eine Cloud von Deutschland für Deutschland. Und jeder, der sie verbessern kann, darf mitmachen.

Der VS-Arbeitsplatz berücksichtigt die typischen Merkmale eines digitalen souveränen Arbeitsplatzes in Behörden-Clouds:

- **Einsatz von Open-Source-Software**: Behörden setzen verstärkt auf Open-Source-Software, die transparenter ist und besser kontrolliert werden kann. Dies reduziert die Abhängigkeit von proprietären Lösungen großer internationaler IT-Unternehmen.

- **Datensouveränität:** Daten werden in eigenen oder nationalen Rechenzentren gespeichert und verwaltet anstatt in ausländischen Cloud-Diensten. Dies schützt die Daten vor fremden, unautorisierten Zugriffen.

- **Sicherheitsstandards**: Strenge Sicherheits- und Datenschutzstandards werden implementiert, um sicherzustellen, dass die IT-Infrastruktur vor Cyberangriffen geschützt ist. Dies umfasst auch regelmäßige Sicherheitsüberprüfungen und -audits.

- **Interoperabilität**: Systeme und Anwendungen werden so entwickelt, dass sie miteinander kompatibel sind und problemlos Daten austauschen können. Dies fördert die Effizienz und Zusammenarbeit zwischen verschiedenen Behörden und Abteilungen.

- **Kontrolle über Software und Hardware**: Behörden haben die Kontrolle über die Software- und Hardware-Komponenten, die sie verwenden. Dies bedeutet, dass sie Anpassungen vornehmen und Sicherheitslücken schließen können, ohne auf externe Anbieter angewiesen zu sein.

- **Vorteile eines digital souveränen Arbeitsplatzes für Behörden:**

  Sicherheit: Durch die Kontrolle über die eigenen Daten und IT-Infrastrukturen können Sicherheitsrisiken besser gemanagt und Cyberangriffe effektiver abgewehrt werden.

  Unabhängigkeit: Behörden sind weniger abhängig von internationalen IT-Dienstleistern und können ihre IT-Strategien unabhängiger gestalten.

  Datenschutz: Die Einhaltung nationaler und europäischer Datenschutzgesetze wird erleichtert, da die Daten innerhalb der eigenen Hoheitsgebiete gespeichert und verarbeitet werden.

  Kostenkontrolle: Langfristig können Kosten eingespart werden, da Open-Source-Lösungen oft kostengünstiger sind und weniger Lizenzgebühren anfallen.

Die National Secure Cloud: Maßgeschneiderte Sicherheit bis zur VS-Einstufung GEHEIM

Sichere und souveräne Cloud-Lösungen sind unverzichtbar in einer modernen IT-Infrastruktur, insbesondere im öffentlichen Sektor. Die National Secure Cloud (NSC) ist eine Antwort auf diese Herausforderung. Sie ist eine flexible und maßgeschneiderte Cloud-Plattform für unterschiedliche Bedarfsträger. Sie passt sich an verschiedene Anforderungen an und erfüllt höchste Sicherheitsstandards.

Modularität und Anpassungsfähigkeit

Die NSC hat eine modulare Struktur. Sie gibt den Bedarfsträgern dadurch einen Baukasten mit maßgeschneiderten Sicherheitslösungen für ihre individuellen Anforderungen. So erhält jeder Anwender – egal ob Behörde oder Militär – eine Lösung, die hinsichtlich Funktionalität und Sicherheit genau auf das jeweilige Einsatzszenario zugeschnitten ist.

Zu den verfügbaren Modulen gehören eine sichere Cloud-Management-Plattform, Software-as-a-Service-Lösungen (SaaS), kryptografische Sicherheitslösungen und vieles mehr – alles auf der Basis europäischer Open-Source-Anwendungen. Die Modularität der NSC ermöglicht auch die Integration neuer Technologien und Anwendungen wie KI-Sprachmodellen oder maschinellem Lernen. Die Cloud kann entsprechend erweitert werden, um diesen Anforderungen gerecht zu werden.

Höchste Sicherheitsstandards gemäß VSA und VS-IT

Im Mittelpunkt der NSC steht die Sicherheit. Sie erfüllt die strengen Anforderungen der Verschlusssachenanweisung (VSA) und der darauf basierenden IT-Richtlinie (VS-IT). Die NSC verwendet Technologien, die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) bis GEHEIM zugelassen oder als zulassungsfähig eingestuft sind. Damit wird sichergestellt, dass die Lösung höchsten Anforderungen an Vertraulichkeit, Integrität und Verfügbarkeit der Daten gerecht wird.

„Jede Cloud benötigt als Herzstück zur Virtualisierung und Ressourcen-Orchestrierung einen Hypervisor", sagt Dr. Michael Hohmuth, Geschäftsführer des NSC-Partners Kernkonzept. „Herkömmliche Clouds nutzen durchweg monolithische Hypervisoren mit umfangreichen Angriffsvektoren. Die NSC hingegen setzt auf den bis zur Geheimhaltungsstufe ‚GEHEIM' zugelassenen, modularen L4Re Secure Separation Kernel, dessen mikrokernbasierte Architektur einen minimalen Angriffsvektor bietet und das Fundament für die Security-by-Design-Strategie der NSC bildet."

Ein weiteres Merkmal ist der Einsatz von Datenverschlüsselung und digitalen Signaturen. Es werden vom BSI zugelassene Hardware-Sicherheitsmodule eingesetzt, die alle verwendeten kryptografischen Schlüssel erstellen, verwalten und aufbewahren. Diese Schlüssel werden zum Beispiel zur Datenverschlüsselung oder Erstellung von Zertifikaten verwendet, sie verlassen aber nie die hochsichere Umgebung des Hardware-Sicherheitsmoduls. Die eingesetzten Sicherheitsmodule sind zudem zukunftssicher und können bei Bedarf auf Post-Quanten-kryptografie (PQC) umgestellt werden.

Sicherheitsdomänen und sichere Übergänge

Die NSC bietet Sicherheitsdomänen an, in denen etwa Behörden oder NATO-Nationen ihre eigene Datenhoheit steuern und Datenverarbeitung sowie -speicherung getrennt durchführen können. Zusätzlich ist die NSC in der Lage, mehrere Sicherheitsdomänen auf der gleichen Server-Hardware zu erstellen und voneinander zu trennen – und zwar bis zum Geheimhaltungsgrad GEHEIM.

Jede Domäne verfügt über spezifische Sicherheitsprotokolle und Zugriffskontrollen. Sie verhindern, dass Informationen ohne entsprechende Berechtigung die Domänengrenzen überschreiten. Diese strikte Trennung schützt vertrauliche Daten militärischer oder staatlicher Organisationen vor unberechtigtem Zugriff. In der Vergangenheit wurden dafür physisch getrennte Systeme verwendet. Mit den neuen Technologien ist es jedoch möglich, mehrere Sicherheitsdomänen verschlüsselt auf einer einzigen Hardwareplattform zu betreiben.

Für den bidirektionalen Datenaustausch zwischen unterschiedlichen Sicherheitsdomänen werden in der NSC SDoT-Produkte (Secure Domain Transition) eingesetzt. „Dadurch können strukturierte und unstrukturierte Daten zwischen den verschiedenen Sicherheitsdomänen ausgetauscht werden, und zwar ebenfalls bis zum Geheimhaltungsgrad GEHEIM", so Benedikt Meng vom NSC-Partner infodas. Dies ist auch im internationalen Kontext wichtig, etwa bei der Zusammenarbeit von NATO-Mitgliedsstaaten. So können zum Beispiel Daten aus einem NATO-SECRET-Bereich sicher an Partnerstaaten übermittelt werden.

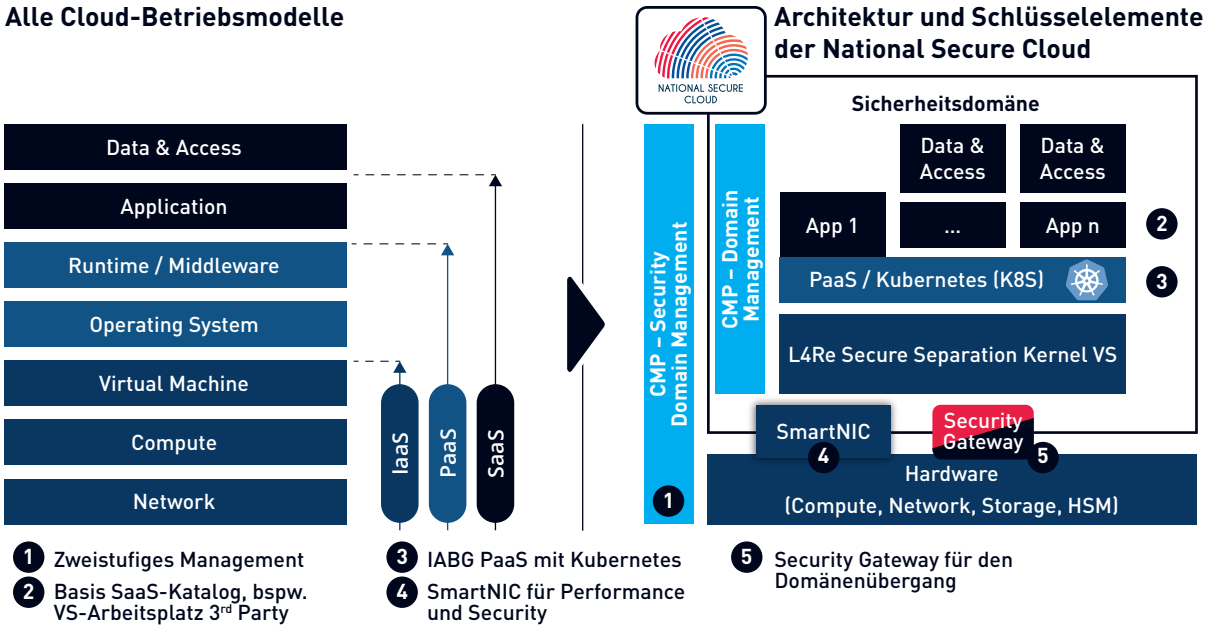
Hohe Interoperabilität und Skalierbarkeit

„Neben den hohen Sicherheitsstandards bietet die NSC Interoperabilität im militärischen und internationalen Umfeld, da sie auf standardisierten und weit verbreiteten Protokollen und Open-Source-Komponenten aufsetzt", ergänzt Nils Gerhardt, Chief Technology Officer beim NSC-Partner Utimaco.

Zudem lässt sich die Cloud leicht in bestehende Infrastrukturen integrieren. Ein weiterer Vorteil ist die Skalierbarkeit. Das Cloud-System kann problemlos an unterschiedliche Bedürfnisse und Einsatzszenarien angepasst werden – auch kurzfristig bei terminabhängigen Spitzenbelastungen.

Die NSC ist als Cloud-Plattform in der Lage, Anwendungen von unterschiedlichen Anbietern zu betreiben. So können Bedarfsträger bereits vorhandene und oft teuer angeschaffte Software weiternutzen und damit ihre Investition schützen. Es ist jedoch empfehlenswert, möglichst bald auf den perfekt mit der NSC harmonisierten VS-Arbeitsplatz (siehe nächste Kapitel) umzusteigen. Er verringert die oft unübersichtliche Software-Vielfalt in den Organisationen und bringt neben mehr Sicherheit auch mehr Effizienz.

Schlüsselelemente der National Secure Cloud



Modular und hochsicher: Der VS-Arbeitsplatz im Detail

Der VS-Arbeitsplatz ist eine moderne Software-Lösung, die sowohl on premise als auch als SaaS (Software as a Service) bereitgestellt wird. Sein Funktionsumfang entspricht den gängigen Office-Produkten der großen Technologiekonzerne. SaaS bedeutet, dass die Software nicht lokal auf einem Rechner installiert ist. Sie befindet sich stattdessen in der Cloud und wird mit einem Browser wie Firefox oder Edge genutzt. Im Fall einer Behörde bedeutet dies, dass der VS-Arbeitsplatz in der Private Cloud eines darauf spezialisierten Anbieters läuft und nicht allgemein über das Internet erreichbar ist. Nur das interne Rechnernetz der jeweiligen Behörde kann darauf zugreifen.

Merkmale des VS-Arbeitsplatzes

Der VS-Arbeitsplatz zeichnet sich durch vier wesentliche Merkmale aus: er ist modular, skalierbar, hochsicher und datensouverän.

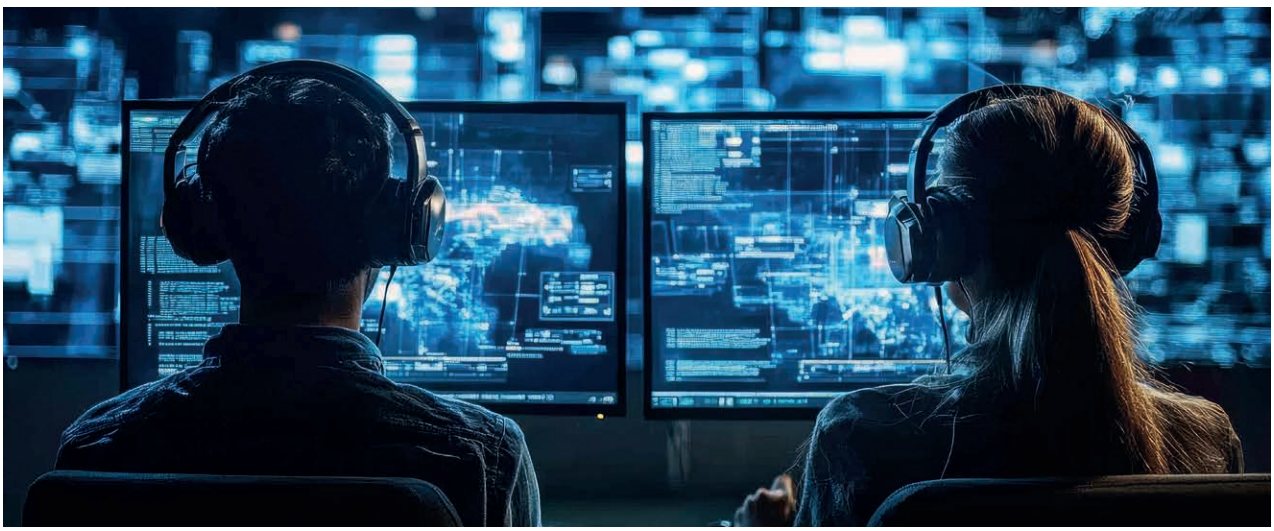
- „Modular" bedeutet: Es handelt sich um bekannte europäische Open-Source-Anwendungen (insbesondere von ownCloud und mspaces), deren Funktionsumfang dem marktgängiger Standardlösungen entspricht. Wo erforderlich, werden die Leistungen weiterer Unternehmen integriert.

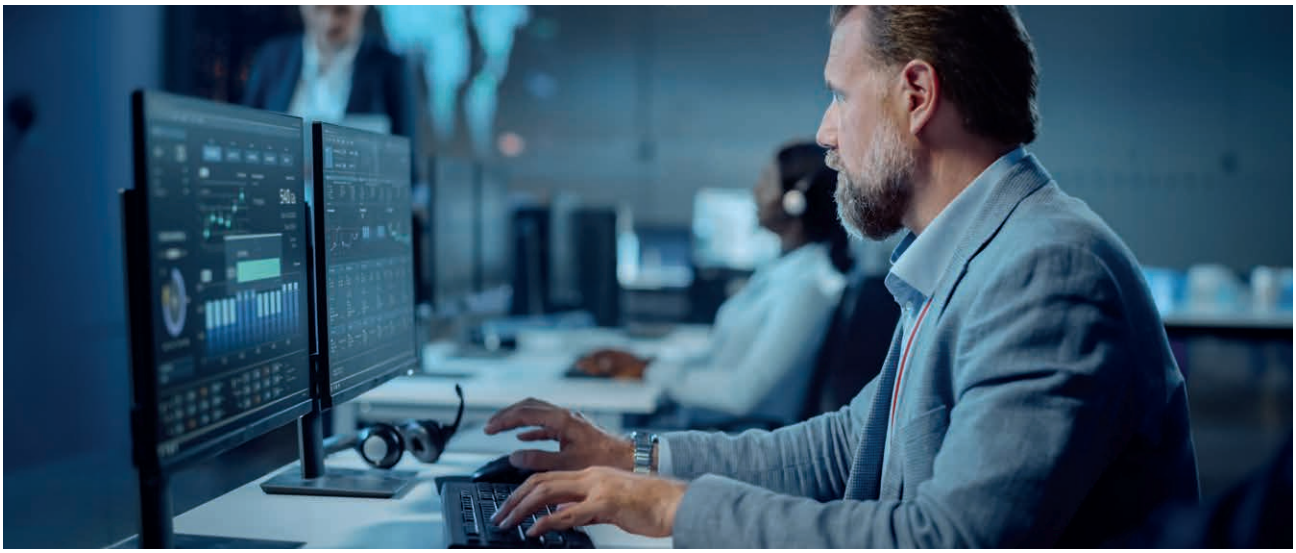
- „Skalierbar" bedeutet, dass die Module des VS-Arbeitsplatzes einzeln für beinahe beliebig viele Benutzer gestartet werden können. Der VS-Arbeitsplatz eignet sich deshalb auch für große Organisationen mit vielen tausend Benutzern.

- „Hochsicher" bedeutet, dass der VS-Arbeitsplatz für die Bearbeitung von Verschlusssachen bis zur VS-Einstufung GEHEIM geeignet ist und alle entsprechenden BSI-Anforderungen unterstützt.

- „Datensouverän" sind alle Cloud-Lösungen und Anwendungen, die den Zugriff auf die Daten ausschließlich dem Nutzer ermöglichen und die Daten in der Heimatregion speichern, in diesem Fall also in Rechenzentren in Deutschland. Für europäische Behörden sind dies speziell zertifizierte Rechenzentren in verschiedenen Ländern.

Synopsis: Der VS-Arbeitsplatz bietet alle gängigen Funktionen moderner Office-Lösungen und garantiert gleichzeitig die Wahrung nationaler Interessen.





Der Zugang zum VS-Arbeitsplatz

Der VS-Arbeitsplatz ist für den Einsatz in einem Browser gedacht, der unter einem BSI-zertifizierten, besonders sicheren Betriebssystem arbeitet. Dieses System ist in der Sprache der IT-Sicherheit „gehärtet", ebenso wie die für den Einsatz in Behörden zertifizierten Laptops oder Desktop-PCs.

Wer den VS-Arbeitsplatz nutzen will, kann ganz einfach einen entsprechenden Link in seinem Browser anklicken oder manuell in die Adresszeile eingeben. Anschließend öffnet sich ein zentrales Portal, in dem alle Funktionen und Module aufrufbar sind.

Damit nur Befugte das Portal nutzen können, ist es durch eine Benutzerverwaltung (Identity and Access Management, IAM) geschützt. Nur Personen, die in der Benutzerverwaltung als berechtigte Anwender registriert sind, können mit ihren Anmeldedaten auf den VS-Arbeitsplatz zugreifen. Dabei gibt es Unterschiede in den Benutzerrechten, sodass nicht jeder auf jedes Modul und jeden Dokumentenbereich zugreifen kann. Ein Beispiel: Wer keine Verschlusssachen bearbeiten darf, hat weder Zugriff auf die entsprechenden Dokumente noch auf die dafür notwendigen Funktionen.

Die Verknüpfung der Benutzer und Berechtigungen erfolgt in einem zentralen Verzeichnisdienst, der Bestandteil des VS-Arbeitsplatzes ist. Er basiert auf der Open-Source-Software Keycloak. Zu den zahlreichen Komfortfunktionen gehört auch die Möglichkeit des Single Sign-on (SSO). Es ermöglicht nach der einmaligen Anmeldung am VS-Arbeitsplatz die automatisierte Anmeldung bei allen weiteren Anwendungen. Darüber hinaus gibt es integrierte User-Self-Services. Mit ihnen kann jeder Benutzer sein Profil und seine Arbeitsumgebung selbst konfigurieren – ohne Hilfe durch den Support.

Der Cloud-Speicher VS-Drive

Eine der Hauptfunktionen des VS-Arbeitsplatzes ist der Cloud-Speicher VS-Drive. Dabei handelt es sich um eine typische Dateiverwaltung im Stil von Dropbox oder OneDrive. Die Benutzeroberfläche ist in den VS-Arbeitsplatz integriert und bietet alle grundlegenden Dateiverwaltungsfunktionen im Windows-Stil.

Die Benutzer können ihre Dateien anzeigen, den Dateityp erkennen, Dateien umbenennen oder löschen. Ebenso können sie beliebig Ordner und Unterordner anlegen, um die eigenen Dokumente zu organisieren.

Darüber hinaus kann jeder Benutzer einzelne Dateien oder Ordner für andere Anwender freigeben. Dabei ist es möglich, die Dokumente oder Ordner nur zum Lesen oder auch zum Bearbeiten freizugeben. Damit ist die gemeinsame Arbeit an Dokumenten möglich. Genutzt wird dafür die integrierte Office-Lösung, die auf den folgenden Seiten vorgestellt wird.

Auch der umgekehrte Weg ist möglich: Jeder kann freigegebene Dateien und Ordner in den eigenen Cloud-Speicher integrieren. Darüber hinaus gibt es öffentlich zugängliche Dateibereiche, in denen beispielsweise Dokumente abgelegt werden, die allen Nutzern zur Verfügung stehen sollen.

Der Dienst basiert auf den entsprechenden Modulen der Open-Source-Lösung ownCloud. Zusätzlich gibt es eine Integration der Office-Lösung, die Teil des VS-Arbeitsplatzes ist.

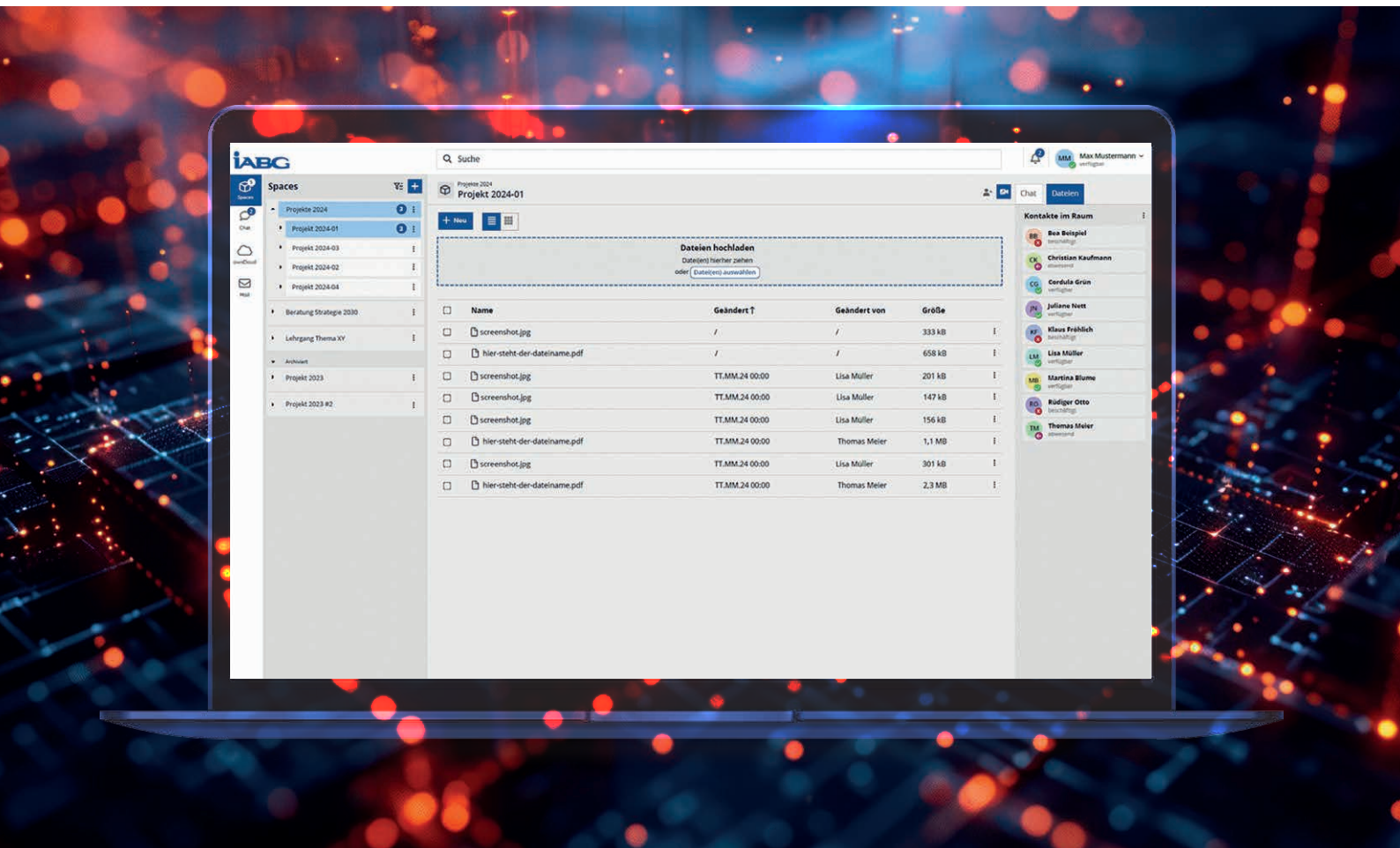
Digitale Zusammenarbeit mit VS-Video und Chat

Videokonferenzen und Chats sind Standardfunktionen moderner Office-Lösungen und damit auch von Collabora Office. Neben Video- und Audiokonferenzen (innerhalb einer Domäne) mit beliebig vielen Teilnehmern gehört dazu auch die Möglichkeit, Bildschirminhalte zu teilen. Damit können Präsentationen, Tabellenkalkulationen oder Dokumente wie gewohnt im Team gezeigt werden.

Darüber hinaus besteht die Möglichkeit, Dokumente auszutauschen und gemeinsam an einem Whiteboard zu arbeiten. Ergänzt wird dies durch einen Text-Chat, an den alle Nutzer des VS-Arbeitsplatzes angeschlossen sind. Diese Funktion der digitalen Zusammenarbeit befindet sich im Modul VS-Realtime. Der Zugriff erfolgt ausschließlich über einen Browser.

Der Kern des VS-Arbeitsplatzes: VS Office Collabora

Das Kernmodul VS Office Collabora ist eine vollständige Office-Anwendung, die VS-Drive als Speicherort für ihre Dokumente verwendet. Die Office-Lösung verfügt über die üblichen Anwendungen für Textverarbeitung, Tabellenkalkulation und Präsentationen. Sie orientieren sich stark an den bekannten Office-Standardlösungen. Deshalb haben sie eine sehr ähnliche Benutzeroberfläche und einen gleichartigen Funktionsumfang.



Der VS-Arbeitsplatz im Vergleich zu der Microsoft Teams Suite

VS-Arbeitsplatz		MS Teams App
VS-Room	**Workspace**	MS Sharepoint
VS-Chat	**Chat**	MS Teams
VS-Video	**Video**	MS Teams
VS-Docs	**Document Processing**	MS Teams
VS-Drive	**Data Platform**	MS oneDrive
VS-ID	**IDM**	AD/LDAP
VS-Base	**Integration Layer**	GraphAPI
NSC (Linux/Windows)	**Platform**	Windows

Das Office-Modul des VS-Arbeitsplatzes unterstützt sowohl die Einzelbearbeitung von Dokumenten als auch die Zusammenarbeit mehrerer Anwender in Echtzeit.

Ein Dokument kann von jedem bearbeitet werden, der Schreibzugriff auf die entsprechende Datei hat. Die Anwendungen können Dokumente im Microsoft-Office-Format (.docx, .xlsx, .pptx) und im Open-Document-Format (ODF) lesen und schreiben. Darüber hinaus unterstützt Collabora viele weitere Dateiformate wie txt, rtf, html, jpg, png, gif, mp4, webM und pdf.

Das Office-Modul des VS-Arbeitsplatzes basiert auf der Open-Source-Cloud-Lösung Collabora Office, die wiederum auf dem Open-Source-Paket LibreOffice basiert und mit Kollaborationsfunktionen erweitert wurde.

Für die Zukunft gerüstet: VS-AI

Das für die nächste Version verfügbare Modul VS-AI erweitert die Funktionen des VS-Arbeitsplatzes um ein Sprachmodell wie das Open-Source-Modell Mistral, das lokal genutzt werden kann. Das Sprachmodell wird kontextuell durch eine zusätzliche, lokale Wissensbasis ergänzt, während es selbst austauschbar bleibt. Auf diese Weise werden unterstützend Dokumentenzusammenfassungen oder Textentwürfe automatisiert möglich.

Die Integration zukunftsweisender Technologien wie KI-Module stellt sicher, dass der VS-Arbeitsplatz langfristig anpassungsfähig bleibt und den Anforderungen wachsender Datenmengen und komplexer Verwaltungsprozesse gerecht wird. Insgesamt schafft die Lösung eine stabile Basis für die digitale Transformation öffentlicher Verwaltungen und eröffnet gleichzeitig Raum für innovative Weiterentwicklungen.

Der VS-Arbeitsplatz wird als Teil der NSC in zwei Abonnementvarianten angeboten: on premise und als SaaS.

- **Geringere Anfangsinvestitionen:** keine hohen Einmalkosten, sondern überschaubare monatliche oder jährliche Zahlungen.
- **Immer aktuelle Software:** Nutzer haben immer Zugriff auf die neuesten Funktionen und Sicherheitsupdates.
- **Flexibilität:** Abonnements können je nach Bedarf skaliert oder angepasst werden.
- **Technischer Support:** kontinuierlicher Zugang zu technischem Support und Hilfe bei Problemen.

Fragen und Antworten zur NSC als Basis des VS-Arbeitsplatzes

Wie hoch ist der Admin-Aufwand für das Deployment der NSC?
Das Deployment folgt dem Industriestandard für Kubernetes im Enterprise-Umfeld. Je nach Größe und verwendeten Modulen im Cluster müssen die sogenannten „Helm Charts" und verbundene Skripte angepasst werden.

Hierfür hat die IABG eine umfassende Sammlung an Vorlagen und viele Beispiele für unterschiedliche Szenarien. Dadurch minimiert sich der Aufwand. Für einen einfachen Cluster müssen lediglich einige Konfigurationswerte geändert werden.

Wie gewährleistet die NSC föderiertes Identity-Management?
Die NSC bietet die Integration des Identity-Managements mit Keycloak. Als „Middleware" kann die Anwendung im Hintergrund unterschiedliche „Identity Provider" anbinden und diese transparent hinter einem Login-Fenster für alle Cloud-Angebote bereithalten. Im Zusammenspiel mit einem Hardware-Sicherheitsmodul (HSM) und Smartcards können Logins auch mit Hardware-Lösungen verbunden werden.

Wie wird in der NSC die Sicherheit für kryptografische Anforderungen gewährleistet?
Es werden umfassende Sicherheitslösungen bereitgestellt, darunter ein vom BSI zugelassenes Hardware-Sicherheitsmodul für alle kryptografischen Anforderungen. Zusätzlich besteht die Möglichkeit, Client-seitigen Schutz durch Festplattenverschlüsselung sowie „File and Folder"-Verschlüsselung bis zum Standard VS-NfD zu nutzen.

Wie garantiert die NSC Skalierbarkeit?
Wir unterscheiden zwischen zwei Aspekten der Skalierbarkeit: horizontal und vertikal. Ersteren adressieren wir mit den üblichen Kubernetes-Techniken (Horizontal Pod Scaler), um das nahtlose Skalieren ohne manuelles Eingreifen zu ermöglichen. Im vertikalen Bereich erlauben wir den Ausbau von Speicher, Prozessoren oder Netzwerkeinheiten.

Ist die NSC bereits abgesichert gegen potenzielle Angriffe von Quantencomputern?
Viele Komponenten sind krypto-agil gestaltet. Sie können bereits heute mit Post-Quanten-Algorithmen aufgerüstet werden. Sobald das BSI diese Komponenten genehmigt, ist die NSC progressiv und quantensicher ausgelegt.

Wie kann man mit der NSC Georedundanz sicherstellen?

Für verlässliche Georedundanz werden drei Kubernetes-Container-Cluster benötigt, die an unterschiedlichen Standorten betrieben werden. Dazu gehört ein „Watchdog"-Prozess, der das Routing der IP-Nummern umstellt, sollte einer der Cluster ausfallen.

Die Rechenzentren können klein sein, da die NSC-Lösung verschiedene Sicherheitsdomänen auf einem Server erlaubt.

Die Rechenzentren sind schnell aufbaubar und die Instanziierung von GEHEIM-Domänen geht schnell.

Information:
Kubernetes-Cluster

Warum braucht es zwei CMPs, um die NSC zu administrieren?

Damit die einzelnen Domänen getrennt bleiben, erfolgt die Administration einer Domäne aus Sicherheitsgründen innerhalb der jeweiligen Domäne. Deshalb gibt es jeweils eine eigene Cloud-Management-Plattform pro Domäne. Davon losgelöst existiert ein übergeordnetes Management, mit dem die einzelnen Domänen erstellt werden können.

Wie stellt man Multi-Mandantenfähigkeit sicher?

Die gesamte Lösung ist mandantenfähig entworfen worden. Durch die logische Kapselung von Kubernetes-Clustern laufen Anwendungen unterschiedlicher Bedarfsträger de facto völlig getrennt voneinander. Dies reicht bis zu den Clients, die auf gekapselten virtuellen Maschinen betrieben werden.

Wie erreicht man mittels der NSC Homogenität im Betrieb über mehrere Standorte hinweg?

Der Technologie-Stack der NSC ist so gestaltet, dass dieselben Technologien vom Cloud-Computing über Fog-Computing bis zum Edge-Computing genutzt werden können. Dadurch wird auch die Administration vereinheitlicht, unabhängig davon, wie groß und umfangreich die Infrastruktur an einem Standort ist.

Welche Vorteile lassen sich durch den Einsatz einer SmartNIC auf Admin-Ebene erzielen?

Durch die SmartNIC können Daten aus mehreren Sicherheitsdomänen, auch mit unterschiedlichen Einstufungen, auf einem einzigen physischen Kabel übertragen werden. Damit entfällt die aufwendige physische Trennung der kompletten Netzwerkinfrastruktur verschiedener Domänen, die mit konventionellen Lösungen notwendig ist. Dadurch lassen sich auch relativ leicht neue Sicherheitsdomänen aufspannen, ohne weitere Hardware zu benötigen.

Was versteht man unter der Multi-Sicherheitsdomänen-Cloud?

Die NSC ist in der Lage, mehrere abgeschlossene Netzwerke oder Domänen für unterschiedliche Geheimhaltungsgrade auf einer Hardware laufen zu lassen und über den L4Re Secure Separation Kernel sicher voneinander zu trennen. Das wurde vom BSI bis zum Geheimhaltungsgrad GEHEIM bestätigt.

Lassen sich zwischen den Sicherheitsdomänen Daten austauschen?

Ja, mit SDoT Security Gateways können strukturierte Daten zwischen den Sicherheitsdomänen ausgetauscht werden. Sie werden dabei von den Gateways anhand eines festgelegten Regelwerks geprüft. Unstrukturierte Daten – etwa Word-, Excel- oder andere Dateien – müssen vor dem Verlassen der Sicherheitsdomäne mittels eines SDoTs gelabelt werden. Auch E-Mails lassen sich auf diesem Weg austauschen. Diese IT-Sicherheitsprodukte sind vom BSI bis zum Geheimhaltungsgrad GEHEIM zugelassen.

Wie ist die Sicherheitsdomäne-as-a-Service realisiert?

Die NSC setzt auf eine physisch-äquivalente Trennung, die überwiegend in Software oder durch flexibel konfigurierbare Hardware-Komponenten umgesetzt wird. Dadurch lassen sich Sicherheitsdomänen schnell erzeugen, ohne dass dafür weitere Hardware nötig ist. Viele Teile sind entweder bereits als Software-Lösung vom BSI bis GEHEIM zugelassen oder setzen auf vom BSI bis GEHEIM zugelassene Hardware-Appliances auf.

Inwieweit ist die NATO-Kompatibilität wie bspw. mit den Federation Mission Networks gegeben?
Die PaaS hat ihren Ursprung in mehr als 14 Jahren Entwicklungserfahrung NATO-konformer Cloud-Anwendungen auf Basis der FMN-Spirals. Ein Beispiel aus dieser Entwicklung sind die Konzepte für das föderierte Identity Management, das unterschiedlichen NATO-Partnern die Zusammenarbeit in gemeinsamen Missionen erlaubt.

Kann ich meine existierenden Anwendungen auf der NSC laufen lassen?
Die NSC nutzt Kubernetes. Da diese Plattform ein De-facto-Standard für neuere Anwendungen ist, lassen sich containerisierte Anwendungen mit minimalem Aufwand auf der NSC betreiben. Unter einigen Linux-Distributionen (Ubuntu, Red Hat Enterprise Linux) können bei Bedarf Legacy-Anwendungen, die nicht in einer containerisierten Umgebung laufen, auch als virtuelle Maschinen innerhalb einer Domäne provisioniert werden.

Worin unterscheidet sich die Architektur der NSC von herkömmlichen Clouds?
Jede Cloud benötigt als Herzstück zur Virtualisierung und Ressourcen-Orchestrierung einen Hypervisor. Im Gegensatz zu herkömmlichen Clouds setzt die NSC auf einen modularen, Mikrokern-basierten Hypervisor. Dieser unterscheidet sich wesentlich von den monolithischen Hypervisoren, die in traditionellen Clouds verwendet werden. Besonders auffällig ist der Unterschied bezüglich der Trusted Computing Base (TCB), der Software und Hardware eines Systems, der man vertrauen muss. Während herkömmliche Clouds auf monolithische Hypervisoren mit Millionen von Codezeilen setzen, besteht die TCB des L4Re Hypervisors in der NSC-Lösung aus lediglich etwa 30.000 Codezeilen. Diese um ein Vielfaches kleinere Codebasis ermöglicht vollständige Überprüfbarkeit und reduziert gleichzeitig die Anfälligkeit für Fehler und Sicherheitslücken.

Wie ist ein BSI-konformer Betrieb mit Virtual Security Functions (VSF) möglich?
Eine Virtual Security Function (VSF) ist eine eigenständige Softwarekomponente, die flexibel und dynamisch auf einem NSC-System je nach Bedarf instanziiert werden kann. Beispiele hierfür sind sichere Netzübergänge mit Labeling-Services oder Kryptografie-Komponenten. VSFs können von verschiedenen Anbietern bereitgestellt und unabhängig voneinander integriert werden. Sie laufen direkt auf dem L4Re Hypervisor, wodurch eine sichere Isolation gewährleistet ist. Bei der Ausfassung einer Sicherheitsdomäne werden VSFs entsprechend den Anforderungen der Domäne gestartet und bieten Sicherheitsfunktionen entweder für die Domäne selbst oder zwischen verschiedenen Domänen.

Wie erfolgt ein sicherer Betrieb der NSC im Hinblick auf Hardware-Risiken wie Spectre und Meltdown?
Die NSC-Architektur implementiert alle notwendigen Schutzmaßnahmen, um sich gegen diese Hardware-Schwachstellen zu schützen. Dabei werden die Domänen des Systems so strukturiert, dass die gemeinsame Nutzung von Ressourcen durch verschiedene Domänen auf ein Minimum reduziert wird. Dies verringert das Risiko für Angriffe wie Spectre oder Meltdown.

Q&A VS-Arbeitsplatz

Was sind die Vorteile eines digital souveränen Arbeitsplatzes für Behörden?

Sicherheit: Durch die Kontrolle über die eigenen Daten und IT-Infrastrukturen werden Sicherheitsrisiken besser gemanagt und Cyberangriffe effektiver abgewehrt.

Unabhängigkeit: Behörden sind weniger abhängig von internationalen IT-Dienstleistern und können ihre IT-Strategien unabhängiger gestalten.

Datenschutz: Die Einhaltung nationaler und europäischer Datenschutzgesetze wird erleichtert, da die Daten innerhalb der eigenen Hoheitsgebiete gespeichert und verarbeitet werden.

Kostenkontrolle: Open-Source-Lösungen sind oft kostengünstiger und haben niedrigere Lizenzgebühren.

Warum nutzen Behörden Open-Source-Software statt der bekannten Standardlösungen?

Behörden setzen verstärkt auf Open-Source-Software, weil sie transparenter ist und besser kontrolliert werden kann. Dies reduziert die Abhängigkeit von proprietären Lösungen großer internationaler IT-Unternehmen. Behörden haben bei Open-Source die Kontrolle über die Software- und Hardware-Komponenten, die sie verwenden. Dies bedeutet, dass sie die Möglichkeit haben, Anpassungen vorzunehmen und Sicherheitslücken zu schließen, ohne auf externe Anbieter angewiesen zu sein.

Was bedeutet der Begriff „Datensouveränität"?

Datensouveränität bedeutet, dass alle Daten in eigenen oder nationalen Rechenzentren gespeichert und verwaltet werden, nicht in ausländischen Cloud-Diensten. Dies schützt die Daten vor unautorisierten Zugriffen. Ergänzend gibt es strenge Sicherheits- und Datenschutzstandards, mit denen die IT-Infrastruktur vor Cyberangriffen geschützt ist. Dies umfasst auch regelmäßige Sicherheitsüberprüfungen und -audits.

Welche Aspekte eines „Arbeitsplatzes" werden von der VS-Arbeitsplatz-Software abgedeckt?

Bereits heute lässt sich der VS-Arbeitsplatz nutzen, um innerhalb einer Domäne per Chat, Videotelefonie, E-Mail oder Dateiaustausch zu kommunizieren. Darüber hinaus sind durch die Integration der SDoT Security Gateways Dateiübertragung und E-Mail-Versand auch über Sicherheitsdomänengrenzen hinweg möglich.

Kann ich mit dem VS-Arbeitsplatz gemeinsam an Dateien arbeiten?

Innerhalb einer Domäne können gängige Office-Formate (Text-Dateien, Tabellen, Präsentationen) innerhalb des Web-Browsers gemeinsam in Echtzeit bearbeitet werden. Anschließend lassen sich Dateien direkt aus derselben Anwendung heraus in eine andere Domäne übertragen.

Lässt sich der VS-Arbeitsplatz auch für die Zusammenarbeit mit internationalen Partnern nutzen?

Der VS-Arbeitsplatz ist für alle in Deutschland genutzten Geheimhaltungsgrade (VS-NUR FÜR DEN DIENSTGEBRAUCH bis GEHEIM) vorgesehen sowie für die äquivalenten NATO-Einstufungsgrade NATO RESTRICTED bis NATO SECRET. Darüber hinaus kann durch den Zusatz „Releasable to" ein eingestuftes Dokument auch an ausgewählte weitere Partnernationen freigegeben werden, sofern zu diesen ein entsprechender Domänenübergang eingerichtet wird.

Wie wird sichergestellt, dass keine GEHEIM eingestuften Daten in eine niedriger eingestufte Sicherheitsdomäne übertragen werden?

Bevor ein Dokument von einer höher eingestuften in eine niedriger eingestufte Domäne übertragen werden kann, muss dieses Dokument mit einem entsprechenden „Label" versehen werden. Das Erzeugen dieses Labels muss stets von einer Person angestoßen werden, die dabei den entsprechenden Geheimhaltungsgrad auswählt. Wird ein Dokument als GEHEIM eingestuft und soll dann in eine niedriger eingestufte Domäne übertragen werden, wird dies vom SDoT Security Gateway unterbunden. Dokumente ohne Label lassen sich grundsätzlich nicht in niedriger eingestufte Domänen übertragen.

Kann ich den VS-Arbeitsplatz an bestehende Identity-and-Access-Management-Systeme anbinden?

Die VS-Arbeitsplatz-Anwendungen nutzen Keycloak als Open-Source-Lösung für das Identitätsmanagement. Dadurch lassen sich existierende Systeme über LDAP oder andere Identity-Provider und Smartcards einbinden.

Wie werden Dateien der Nutzer in der Cloud verwaltet?

Grundlage der Dateiverwaltung ist das bekannte Open-Source-Produkt „oCIS" der Firma ownCloud. Diese Software wird von Industrie und öffentlicher Hand (von Mercedes über Bayercloud bis CERN) für Dateiverwaltung und Skalierung im Enterprise-Umfeld unterstützt und eingesetzt. So existieren erprobte Versionierung, automatische Sicherung und viele andere Enterprise-Funktionen automatisch auch für den VS-Arbeitsplatz.

Ausblick – Wir gestalten Sicherheit, gemeinsam

Wir verstehen die Verschlusssachenanweisung (VSA) als wichtigen Innovationstreiber. Das bedeutet für uns beständiger Fortschritt. Dabei wollen wir mit unseren technischen Weiter- und Neuentwicklungen künftigen Cyberbedrohungen voraus sein. Es geht uns darum, Sicherheitsstandards nicht nur zu nutzen, sondern sie zu härten und zu gestalten.

Orientierung an den Anforderungen der Bedarfsträger

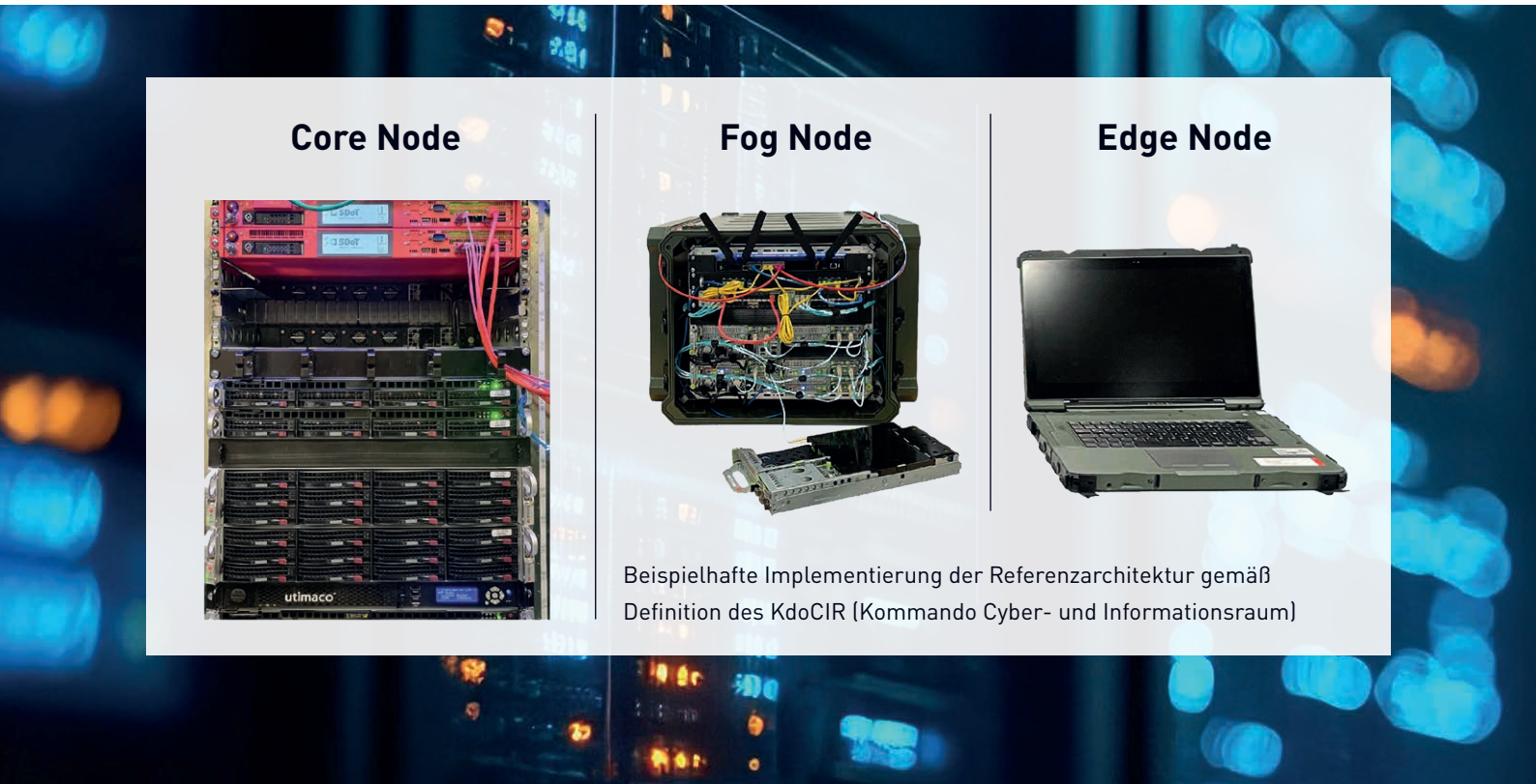
IT-Sicherheit und digitale Souveränität – und damit Handlungsfähigkeit für Staat und Gesellschaft – kommen für uns vor „Look & Feel". Unser Partnernetzwerk aus vertrauenswürdigen deutschen Unternehmen zeigt mit seinen zugelassenen Komponenten bereits heute, wie man die anspruchsvollen Anforderungen der VSA auch jenseits von VS-NfD angeht: konstruktiv und ressourcenschonend, transparent und nachvollziehbar.

Wir zeigen außerdem, dass ein VS-fähiger Arbeitsplatz den Anforderungen der modernen digitalen Zusammenarbeit standhält und Austausch und Kommunikation fördert – ohne von großen Software-Anbietern abhängig zu sein. Unsere Nutzer tappen damit nicht in die Falle des Vendor-Lock-in.

Wir verstehen, dass Hardware und Software künftig zu trennen sind. Unser modularer Ansatz ermöglicht die komfortable Integration von Drittanbietern. Ist deren Software Kubernetes-fähig, dann ist schon viel gewonnen.

Die Zulassungsverfahren stellen hohe Anforderungen an alle beteiligten Akteure. Die Orientierung am Wirkungsdreieck Bedarfsträger, Zulassungsstelle und Dienstleister ist Voraussetzung dafür, IT-Sicherheit und digitale Souveränität für Deutschland zu erreichen und dauerhaft zu sichern – ressourcenschonende und wirtschaftliche Umsetzung immer im Blick.

Mit dem NSC-Demonstrator können MDCC-Szenarien im Kontext von MDO bereits heute verprobt und Mehrwerte nachgewiesen werden.



Beispielhafte Implementierung der Referenzarchitektur gemäß Definition des KdoCIR (Kommando Cyber- und Informationsraum)

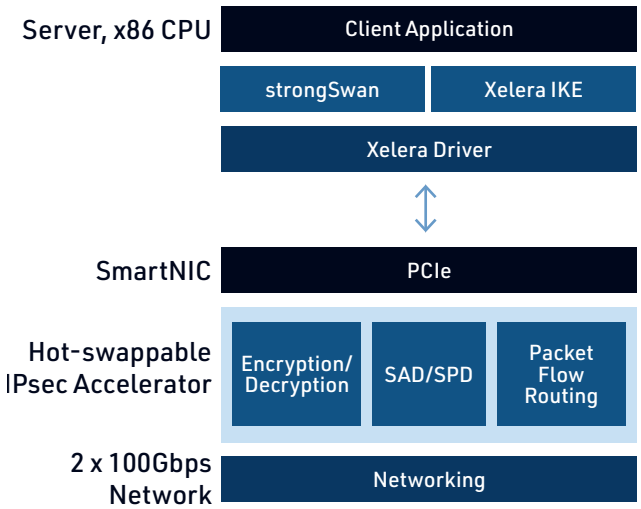
Einfache Integration neuer Technologien

Um die Skalierbarkeit, Flexibilität und Wirtschaftlichkeit der NSC kontinuierlich auszubauen, gibt es aufeinander folgende Stufen, von denen einige bereits in der Entwicklung sind.

Ein Beispiel ist die Integration der SmartNIC-Technologie. Im Gegensatz zu konventionellen Cloud-Lösungen im zugelassenen Sicherheitskontext verzichtet SmartNIC auf die physische Trennung der Netzwerkinfrastruktur verschiedener Sicherheitsdomänen. Sie vervollständigt so das Konzept der NSC, mehrere Sicherheitsdomänen auf einer Hardware zu betreiben. Damit erhöht SmartNIC die Skalierbarkeit der NSC und ermöglicht eine flexible Verwaltung der Sicherheitsdomänen. Mit 100 Gbps Datendurchsatz gewährleistet sie eine Leistung der Netzwerk- und Verschlüsselungsinfrastruktur, die modernen, kommerziellen Cloud-Infrastrukturen entspricht.

Aufgrund ihrer Programmierbarkeit ist sie ein integraler Bestandteil des Sicherheitskonzeptes der künftigen NSC, in dem Weiterentwicklungen ohne den Austausch von Hardware abgebildet werden. Die SmartNIC-Integration erfolgt in Zusammenarbeit mit dem Partnerunternehmen Xelera Technologies GmbH.

Aufbau SmartNIC: Zoom-in aus Abb. Seite 13



Flexibel dank eines starken Partnernetzwerks

Unser deutsches Partnernetzwerk ist der Beginn eines offenen und stabilen Ökosystems. Es ist geprägt vom Gedanken an Modularität, Flexibilität und Interoperabilität. So werden mit der Zeit zugelassene IT-Sicherheitskomponenten, die eine Hardware als Vertrauensanker haben, mehr und mehr durch Softwarekomponenten ersetzt. Die Entwicklungs-Roadmaps der Partner weisen bereits den Weg dafür.

Wir kommen dem Wunsch der Bedarfsträger nach einer echten, kontrollierbaren „Sicherheitsdomäne as a Service“ nach. Sie erlaubt dynamisches Einrichten und Administrieren in Minuten statt Stunden oder Tagen.

Die Zukunft der NSC ist dynamisch

Heute ist unsere NSC statisch und funktional. Sie genügt den Zulassungsanforderungen und bildet die Basis, um die aktuellen Szenarien der Bedarfsträger in zivilen wie militärischen Bereichen sicherheitskonform zu bedienen.

In Zukunft ist die NSC dynamisch – nicht nur für Deutschland. Davon profitieren Administratoren: Sie können immer komplexere Anforderungen ressourcenschonend umsetzen, mit allen Sicherheitsanforderungen und -standards.

Der konsequente Einsatz von Open-Source-Software bedeutet Flexibilität und Unabhängigkeit. Die Administratoren stellen den Betrieb sicher und wehren Cyberattacken ab. Die Anwender konzentrieren sich mithilfe des VS-Arbeitsplatzes auf die Bewältigung der zunehmenden Zahl sicherheitsrelevanter Aufgaben. Sie werden dabei nicht mit der technischen Komplexität konfrontiert. Kurzum: Wir gestalten Sicherheit, gemeinsam – gemeinsam mit Bedarfsträgern und den zulassenden Stellen, und schaffen so Vertrauen und Akzeptanz.

Die Partnerunternehmen des NSC-Programms

Die National Secure Cloud (NSC) wird im Verbund unterschiedlicher deutscher Unternehmen entwickelt. Jedes Mitglied übernimmt dabei spezifische Aufgaben, um den strengen Anforderungen des öffentlichen Sektors, des Militärs und regulierter Industrien gerecht zu werden.

infodas
connect more. be secure.

infodas zählt zu den führenden Lösungsanbietern für Cyber- und Informationssicherheit in Deutschland. Seit 2024 ist die infodas ein Airbus-Tochterunternehmen. Neben der Beratung von Unternehmen, Behörden und Streitkräften entwickelt infodas Hochsicherheitsprodukte für Domänenübergänge sowie den Schutz kritischer Infrastrukturen. Die SDoT-Produktfamilie (Secure Domain Transition) der infodas ist für die Geheimhaltungsgrade GEHEIM, EU SECRET und NATO SECRET zugelassen. Die Produkte sind nach Common Criteria zertifiziert und weisen weitere länderspezifische Zertifikate auf.

Sie umfassen eine Reihe von Security Appliances zum kontrollierten unidirektionalen oder bidirektionalen Datenaustausch zwischen Netzwerken/Systemen von unterschiedlicher Sensitivität sowie dem Erstellen von NATO STANAG 4774/8 konformen und hochsicheren Security Labeln für Daten. Diese Funktionen sind essenziell für den Datenaustausch in einer Cloud mit mehreren Sicherheitsdomänen, um den Informationsaustausch zwischen Behörden oder Nationen zu gewährleisten.

utimaco®

Utimaco leistet einen wichtigen Beitrag für alle kryptografischen Anforderungen mittels eines vom BSI zugelassenen Hardware-Sicherheitsmoduls, welches die physische Sicherheit der NSC-Schlüssel gewährleistet. Optional liefert Utimaco weiteren Client-seitigen Schutz mit Festplattenverschlüsselung und „File and Folder"-Verschlüsselung bis VS-NfD.

Utimaco ist ein globaler Plattformanbieter vertrauenswürdiger Lösungen und Dienstleistungen für Cybersicherheit und Compliance. Wir entwickeln lokale und cloudbasierte Hardware-Sicherheitsmodule, Lösungen für Schlüsselmanagement, Datenschutz und Data-Intelligence-Lösungen für regulierte kritische Infrastrukturen und öffentliche Warnsysteme.

Utimaco ist einer der weltweit führenden Hersteller in seinen wichtigsten Marktsegmenten, mit umfangreichen Kompetenzen und Erfahrungen aufgrund der mehr als 40-jährigen Tätigkeit im Bereich der IT-Sicherheit. Utimaco ist vom BSI „qualifizierter Hersteller" für Hardware-Sicherheitsmodule.

INFODAS GmbH
Rhonestraße 2
50765 Köln

Benedikt Meng
Business Development
& Public Affairs
b.meng@infodas.de
+49 30 2060 3994 51
www.infodas.com

Utimaco IS GmbH
Germanusstraße 4
52080 Aachen

Nils Gerhardt
Chief Technology Officer
nils.gerhardt@
utimaco.com
+49 241 1696 232
www.utimaco.com

KERNKONZEPT

Kernkonzept ist ein Spezialist für hochsichere Betriebssystemlösungen und entwickelt auf Basis des Open-Source-Betriebssystems L4Re sowie des L4Re Hypervisors fortschrittliche Virtualisierungstechnologien für die NSC. Mit diesen Lösungen können Organisationen mehrere Sicherheitsdomänen mit unterschiedlichen Einstufungen sicher auf einer einzigen Hardwareplattform betreiben.

Das L4Re Operating System Framework basiert auf einer Mikrokern-Architektur. Dadurch werden sicherheitskritische Anwendungen strikt von Standardanwendungen getrennt, was das Risiko für Sicherheitslücken erheblich verringert. Die L4Re-Technologie bietet nicht nur ein Höchstmaß an Flexibilität und Effizienz, sondern ist auch vom Bundesamt für Sicherheit in der Informationstechnik (BSI) für die Verarbeitung von bis zu als GEHEIM klassifizierten Daten zugelassen. Sie wird bereits in sicherheitskritischen Umgebungen wie Regierungs-Laptops und Netzwerktechnik eingesetzt und gewährleistet den sicheren Umgang mit als GEHEIM, NATO SECRET und EU SECRET eingestuften Informationen.

XELERA

Die Xelera Technologies GmbH ist ein 2018 gegründetes Softwareunternehmen mit Sitz in Deutschland. Es bietet leistungsstarke KI- und Cybersicherheitsprodukte für Rechenzentren und Cloud-Umgebungen für Kunden in Europa, den USA und Australien. Das Unternehmen verfügt über Kernkompetenzen in den Bereichen SmartNIC/DPU und Netzwerktechnologie.

Xelera ermöglicht Clouds und Rechenzentren der nächsten Generation, um die Anforderungen an die Datenrate zu erfüllen. Xelera bietet SmartNIC- und KI-Infrastrukturtechnologie.

Die SmartNIC/DPU-Software spielt eine entscheidende Rolle bei der Optimierung von Leistung und Kosteneffizienz in Rechenzentren, was für die nächste Generation von KI-Anwendungen wichtig sein wird. Unsere Technologie reduziert den Stromverbrauch von Servern in Rechenzentren erheblich.

Kernkonzept GmbH
Buchenstraße 16b
01097 Dresden

Dr. Michael Hohmuth
CEO
michael.hohmuth@
kernkonzept.com
+49 351 41 888 611
www.kernkonzept.com

Xelera Technologies GmbH
Rheinstraße 40-42
64283 Darmstadt

Felix Winterstein
CEO
felix.winterstein@
xelera.io
+49 6151 6290901
www.xelera.io

GLOSSAR

Datensouveränität
Kontrolle über die eigenen Daten. Der Nutzer bestimmt, wer wie und zu welchem Zweck auf seine Daten zugreifen kann und wie diese verarbeitet werden.

Gehärtetes System
Ein speziell gesichertes IT-System, das durch Maßnahmen wie das Entfernen unnötiger Funktionen und das Schließen von Sicherheitslücken widerstandsfähiger gemacht wurde.

Hypervisor (Mikrokern-basiertes Betriebssystem)
Software, die den gleichzeitigen Betrieb mehrerer virtueller Maschinen auf einer physischen Maschine ermöglicht, indem sie Hardwareressourcen effizient aufteilt. Zudem setzt ein Hypervisor eine strenge Separierung zwischen Domänen durch.

Infrastructure as a Service (IaaS)
Das Cloud-Computing-Modell stellt IT-Ressourcen wie Rechenleistung, Speicher und Netzwerke als Service bereit. Die Nutzer betreiben darauf ihre eigenen Anwendungen.

IoT (Internet of Things)
Ein Netzwerk physischer Objekte, die mit Sensoren, Software und Konnektivität ausgestattet sind, um Daten zu erfassen und auszutauschen.

Security by Design
Sicherheitsmaßnahmen werden von Anfang an in den Entwicklungsprozess von Systemen oder Anwendungen integriert, um Schwachstellen zu minimieren.

Sicherheitsdomäne
Ein isolierter Bereich in einem IT-System, der auf eine bestimmte Sicherheitsstufe ausgelegt ist. Innerhalb der Domäne gelten strikte Zugriffsregeln für die Verarbeitung von Daten.

Single Sign-on (SSO)
Ein Authentifizierungsverfahren, bei dem Nutzer sich einmalig anmelden und dann Zugriff auf verschiedene Anwendungen oder Systeme haben – ohne sich erneut authentifizieren zu müssen.

SmartNIC
Besondere Form der Netzwerkschnittstellenkarte zur Entlastung der Server-CPU von der Netzwerkverarbeitung. SmartNICs können u. a. Aufgaben wie Netzwerkkomprimierung und -dekomprimierung sowie Ver- und Entschlüsselung auslagern.

Software as a Service (SaaS)
Das Cloud-Computing-Modell stellt Software über das Internet als Dienst bereit. Nutzer greifen per Webbrowser darauf zu, ohne die Software lokal installieren zu müssen.

Verschlusssachen (VS)
Angelegenheiten und Sachen aller Art, die durch besondere Sicherheitsmaßnahmen gegen die Kenntnis durch Unbefugte geschützt werden müssen. Sie werden entsprechend ihrer Schutzwürdigkeit als STRENG GEHEIM, GEHEIM, VS-VERTRAULICH oder VS-NUR FÜR DEN DIENSTGEBRAUCH von einer amtlichen Stelle oder auf deren Veranlassung eingestuft.

VS-Daten
Geheimhaltungsbedürftige Informationen, die zur maschinellen Verarbeitung in spezifischer Form dargestellt oder verarbeitet werden bzw. einem solchen Prozess entstammen (USB-Sticks, Festplatten o. Ä.).

Weitere Informationen:
Öffentlicher Sektor – IABG

IMPRESSUM

Verantwortlich
Industrieanlagen-Betriebsgesellschaft mbH
85521 Ottobrunn
Tel.: +49 89 6088 0
info@iabg.de
www.iabg.de

Inhaltlich
Industrieanlagen-Betriebsgesellschaft mbH
Einsteinstraße 20
85521 Ottobrunn

INFODAS GmbH
Rhonestraße 2
50765 Köln

Kernkonzept GmbH
Buchenstraße 16b
01097 Dresden

Utimaco IS GmbH
Germanusstraße 4
52080 Aachen

Xelera Technologies GmbH
Rheinstraße 40-42
64283 Darmstadt

Redaktionelle Gestaltung
Thöring & Stuhr Kommunikationsberatung GmbH
Mittelweg 144
20148 Hamburg

Gestaltung
CC.CONSTRUCT GmbH & Co. KG
Hofaue 21
42103 Wuppertal

Druck
Rapp-Druck GmbH
Kufsteiner Straße 101
83126 Flintsbach

IABG | infodas | KERNKONZEPT | utimaco® | XELERA

Sicherheit ist nicht verhandelbar.

www.iabg.de