Beitrag des Fraunhofer IPT zum Konsultationsprozess zur nationalen Rechenzentrumsstrategie

Ausgangslage und Motivation

Die Bedrohung durch Cyberkriminalität nimmt ständig zu. Unternehmen und Forschungseinrichtungen sind immer häufiger Ziel von Hackerangriffen, die zu erheblichen finanziellen Verlusten, Datenverlusten und Schäden an der Reputation führen können. Im Jahr 2024 waren mindestens 81% der Unternehmen in Deutschland von Datendiebstahl, Spionage oder Sabotage betroffen. [1,2] Es ist daher von größter Bedeutung, die IT-Sicherheitsmaßnahmen kontinuierlich zu verbessern und anzupassen. Auf der anderen Seite legen Kunden von Forschungseinrichtungen zunehmend Wert auf die Sicherheit ihrer Daten. Das Vertrauen, dass ihre sensiblen Informationen geschützt sind, ist ein entscheidender Faktor für die Kundenzufriedenheit und langfristige Geschäftsbeziehungen. Dazu gehört auch, dass die Daten am Standort der Forschungseinrichtung gespeichert werden und nicht an Dritte zur Verarbeitung weitergeleitet werden. Ebenso unterliegen Forschungsdaten strengen Anforderungen durch Fördergeber, bürokratische Vorschriften und Kundenaufträge. Die Einhaltung dieser Anforderungen ist unerlässlich, um die Integrität und Verlässlichkeit der Forschungsdaten zu gewährleisten. Es ist daher notwendig, sowohl die IT-Sicherheit als auch die IT-Souveränität zu stärken und entsprechende Maßnahmen zu ergreifen, um den Kundenanforderungen gerecht zu werden.

Dabei steigen die Kosten für IT-Lösungen, insbesondere für den Bereich IT-Sicherheit, Lizenzkosten, kontinuierlich [3]. Dies stellt eine finanzielle Belastung für Forschungseinrichtungen dar, die auf aktuelle und leistungsfähige IT-Systeme angewiesen sind. Insbesondere betrifft dies kleinere oder Einzelfoschungseinrichtungen, die nicht in der Lage sind, Synergien mit größeren Forschungsverbünden zu heben. So verfügt jedes Institut über seine eigene dezentrale IT-Infrastruktur, sei es ein einzelnes Fraunhofer-Institut oder ein RWTH-An-Institut. Die über viele Jahre gewachsene Struktur der Institute, die stark von institutsindividuellen Optimierungszielen und lokalen Restriktionen geprägt ist, erweist sich insgesamt aus ökonomischer und ökologischer Perspektive als ineffizient. Eine nachhaltige Optimierung erfordert daher ein abgestimmtes Vorgehen der Institute, verbunden mit einer erheblichen Anfangsinvestition.

Um den zunehmenden Bedrohungen durch Cyberkriminalität, den steigenden Kosten für IT-Lösungen und den strengen Anforderungen an Forschungsdaten gerecht zu werden, ist es erforderlich, in einem gemeinsamen Leuchtturmprojekt zusammenzuarbeiten und die Herausforderungen gemeinsam anzugehen. Die dafür nötigen Fördermittel ermöglichen es, die IT-Sicherheit zu verbessern, die IT-Infrastruktur auszubauen und den Anforderungen der Kunden und Fördergeber gerecht zu werden. Nur so können die Innovationskraft und Wettbewerbsfähigkeit der Forschungseinrichtungen und Unternehmen langfristig gesichert werden.

Aufbau zukunftsfähiger und leistungsstarker Rechenzentrumsstandort für anwendungsnahe Forschungseinrichtungen

In diesem Konzept soll ein hochmodernes IT-Security Center für anwendungsnahe Forschungseinrichtungen aufgebaut werden. Dieses Zentrum soll als Vorbild und als Blaupause für andere außeruniversitäre Institute dienen. Darüber hinaus soll eine Übertragbarkeit auf KMUs gezeigt werden.

Das IT-Security Center wird so aufgebaut, dass es die Resilienz der Forschungseinrichtungen nachhaltig stärken und die Umsetzung der NIS2-Richtlinie vorantreiben wird, um die Cybersicherheit bestmöglich nach aktuellem Stand-der-Technik und darüber hinaus zu gewährleisten. Zudem wird das Prinzip der GreenIT evaluiert und überall dort implementiert, wo es ökonomisch und ökologisch sinnvoll ist. Damit wird die Nachhaltigkeit der IT-Infrastruktur gefördert und ein Beitrag zum Umweltschutz geleitet.

Folgende Technologien sollen im zentralisierten IT Security Center etabliert werden:

- **Security Information and Event Management (SIEM)-Lösungen** zur frühzeitigen Erkennung von Cyberangriffen und Datenabflüssen. SIEM-Systeme ermöglichen die zentrale Überwachung und Analyse sicherheitsrelevanter Ereignisse und tragen maßgeblich zur Erhöhung des Schutzes vor aktuellen Bedrohungen bei.
- **Standardisierte Provisionierung von virtuellen Maschinen (VMs)** mittels eines „Datacenter in a Box"-Konzepts. Diese Lösung erlaubt es den angeschlossenen Forschungseinrichtungen, leistungsfähige und sichere IT-Ressourcen direkt am Ort der Datengenerierung flexibel bereitzustellen und so die lokale Verarbeitung sensibler Forschungsdaten gemäß aktuellen Sicherheitsstandards zu gewährleisten.
- **Zentrales Storage- und Backup-System** zur konsolidierten Speicherung und Sicherung der Forschungsdaten. Durch die gemeinsame Nutzung von Speicher- und Backup-Infrastruktur werden sowohl die Ausfallsicherheit als auch die effiziente Nutzung der vorhandenen Ressourcen erhöht. Die zentrale Datenhaltung ermöglicht zudem eine einheitliche Umsetzung von Datenschutz- und Compliance-Anforderungen sowie eine schnelle Wiederherstellung im Notfall.

Ein weiterer Bestandteil des IT-Security Centers wird die Ausbildung und Beschäftigung von IT-Auszubildenden sein. Durch diese zentrale Ausbildungsstätte mit vielfältigen Kompetenzen wird nicht nur die Nachwuchsförderung im IT-Bereich gestärkt, sondern auch eine praxisnahe und qualitativ hochwertige Ausbildung garantiert. Dies wird die dringend benötigten Fachkräfte von morgen optimal vorbereiten und ihnen den Einstieg in die Berufswelt erleichtern.

Darüber hinaus werden im IT-Security Center regelmäßige Schulungen und Workshops angeboten. Diese sollen nicht nur den Wissenstransfer innerhalb des Zentrums fördern, sondern auch Unternehmen und andere Forschungseinrichtungen erreichen. Durch diese Workshops und Schulungen wird das Know-how effektiv weitergegeben, sodass auch externe Partner von den Fortschritten und Erkenntnissen profitieren können. Dies trägt maßgeblich zur Verbesserung der IT-Sicherheitsstandards und zur langfristigen Sicherstellung der Innovationskraft bei.

Wir beabsichtigen zudem, die Übertragbarkeit der entwickelten Lösung auf kleine und mittlere Unternehmen (KMU) systematisch zu untersuchen. KMU stehen vor vergleichbaren Herausforderungen wie Einzelforschungseinrichtungen, insbesondere im Hinblick auf die hohen Anforderungen an eine moderne IT-Infrastruktur. Häufig können diese Anforderungen aufgrund begrenzter personeller und finanzieller Ressourcen nicht adäquat erfüllt werden. Die Möglichkeit, das IT-Security Center auf KMU-Netzwerke oder -Verbünde zu übertragen, bietet daher einen signifikanten Mehrwert: Durch die Bündelung von Ressourcen und den Zugang zu

zentralisierten Sicherheitslösungen können Wettbewerbsfähigkeit gestärkt und Kosten gesenkt werden.

Durch die Kombination von praxisnaher Forschung, sicherer und nachhaltiger IT-Infrastruktur und umfassender Ausbildung wird das IT-Security Center zu einem unverzichtbaren Bestandteil der regionalen und nationalen Forschungslandschaft.

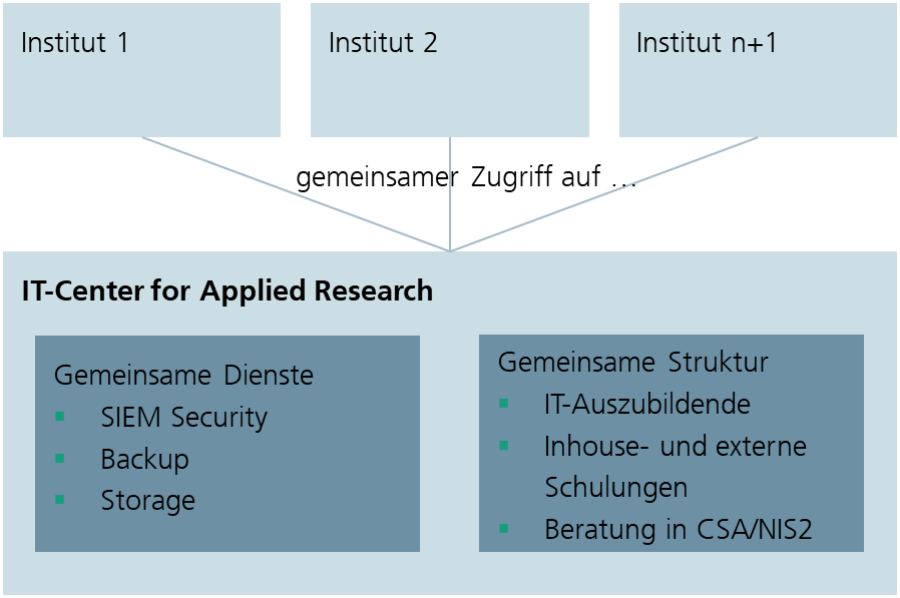

Abbildung 1: Zielstruktur der Investition

Referenzen:
[1]: BSI: Die Lage der IT-Sicherheit in Deutschland, https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html
[2]: BKA: Bundeslagebild Cybercrime 2024: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2024.pdf?__blob=publicationFile&v=3
[3]: VOICE: IT-Agenda 2025: IT-Agenda 2025: Kostendruck auf IT-Organisationen steigt weiter – Budgeterhöhungen reichen nicht aus - VOICE