Matcht Bare.ID die Digitalstrategie des Bundes?

Tolleiv Nietsch - 2024-09-16 - Fragen zum Produkt

Die Digitalstrategie des Bundes wird überarbeitet und legt den Fokus auf digitale Souveränität – Ein Aspekt der für Bare.ID schon heute selbstverständlich ist

Cyberangriffe und die damit einhergehenden Risiken sind gerade in Krisenzeiten so präsent wie nie: Sowohl Corona als auch der Krieg gegen die Ukraine haben gezeigt, wie dringend die Digitalisierung in öffentlichen Einrichtungen und KRITIS-Bereichen ist, aber gleichzeitig auch wie oft gerade diese Stellen Ziel von Cyberangriffen werden.

Die fortlaufend steigende Gefahr Ziel eines Cyberangriffs zu werden erklärt den erhöhten Bedarf, dass jede Digitalisierungsstrategie auch mit einer umfangreichen Cybersecurity-Strategie einhergehen muss. Je mehr Geschäftsprozesse und Daten digital abgebildet werden, desto höher die Angriffsfläche und der Bedarf adäquater sicherheitsrelevanter Lösungen. Grundsätzlich haben hier amerikanische Digitalunternehmen aufgrund ihrer Fortschrittlichkeit eine dominante Stellung bei der Gestaltung der Digitalisierung im europäischen Raum. Um eine Abhängigkeit von diesen nicht-europäischen Anbietern zu verhindern und den deutlich höheren Datensicherheitsstandards im deutschen bzw. europäischen Raum gerecht zu werden wird deshalb von Bundesebene eine Förderung der heimischen Wirtschaft, v.a. im Cloud-Umfeld, verlangt.

Mit der internationalen Digitalstrategie der Bundesregierung Deutschland wird somit auch das Thema Security und digitale Souveränität in den Vordergrund gestellt. Die Strategie wird von verschiedenen Stakeholdern in beratender Funktion begleitet, so auch vom Bundesverband IT-Mittelstand e.V. (BITMi), in welchem Bare.ID Mitglied ist. Erst kürzlich gab BITMi in einer aktuellen Pressemeldung nähere Infos über die Kernziele der beratenden Funktion bekannt. Die Problematik der Abhängigkeit von Drittstaaten durch ausländische Mehrheitsanteile ist auch im Umfeld von Single Sign-On Cloud Lösungen keine Unbekannte, weshalb die Cloud IAM Lösung Bare.ID bereits mit Gründung den Schwerpunkt auf digitale Souveränität gesetzt und sich Compliance zum USP gemacht hat. Wie digitale Souveränität vollumfänglich realisiert werden kann und wie Bare.ID diese umsetzt und somit die Digitalstrategie des Bundes verfolgt, greifen wir im Nachfolgenden auf.

Digitale Souveränität: Was muss gewährleistet sein?

Um digitale Souveränität abzubilden und somit Abhängigkeiten zu minimieren spielen verschiedene Faktoren eine Rolle, sowohl geografisch als auch technologisch. Geografisch soll eine Abhängigkeit von Drittstaaten, welche wie erwähnt im digitalen Umfeld noch stark gegeben ist, stark reduziert werden. Dies geschieht allerdings nicht nur über nationale Anbieter mit dem Gütesiegel „Made in Germany“, welches ausschließliche Herkunft und Standort bestimmt, sondern die Umsetzung digitaler Souveränität bedeutet weit aus mehr und zwar, dass auch die gesellschaftsrechtliche Kontrolle zu jeder Zeit in Deutschland bleibt. Im Zweifelsfall spielt es keine Rolle, ob die Verarbeitung in einem Rechenzentrum auf Schweizer oder europäischen bzw. deutschen Boden stattfindet – entscheidend ist, welcher Rechtsprechung der Anbieter durch seine Herkunft unterliegt. Digitale Souveränität ist erst dann gegeben, wenn es Sperrminoritäten und somit keine Mehrheitsanteile für nicht deutsche Anteilseigner gibt. Ein weiterer Aspekt hierbei, welcher häufig übersehen wird, ist die Betrachtung der Lieferkette. Auch wenn der Anbieter selbst auf alle Standards und Regularien achten, blockiert eine Abhängigkeit von nicht-deutschen Software Lieferanten die vollständige Souveränität. Um digitale Souveränität zu realisieren, muss auch diese die entsprechenden Kriterien erfüllen.

Neben dem geografischen Aspekt spielt auch die Datenverfügbarkeit eine Rolle. Zum einen muss seitens der Anbieter bzw. Lösungen sichergestellt sein, dass die Verfügbarkeit bzw. der Zugang selbst im Krisenfall gewährleistet ist. Das bedeutet, dass Redundanzen geschaffen werden müssen, damit bei einem Ausfall eines Teil des Systems ein anderer Teil dessen Aufgaben übernehmen kann, bis er wiederhergestellt oder ersetzt ist. Hochverfügbarkeit trägt auch zur Skalierbarkeit bei, da sie ein einfaches Wachstum nach Bedarf ermöglicht. Dies erleichtert es Unternehmen, sich bei unerwarteten Änderungen oder Nachfragespitzen schnell anzupassen. Zum anderen wird die einfache Datenportabilität relevant: Eine Abhängigkeit von einzelnen Anbietern, also ein Vendor Lock-In, soll vermieden werden. Als Vendor Lock-in bezeichnet man die Situation, in der ein Kunde nicht in der Lage oder nicht willens ist, von einem bestimmten Anbieter weg zu migrieren, sei es aufgrund vertraglicher Verpflichtungen oder anderer Faktoren wie dem Mangel an kompatiblen Systemen anderer Anbieter oder der Angst vor Unterbrechungen aufgrund von Migrationsprozessen. Durch die Vermeidung einer Anbieterbindung können Unternehmen den Anbieter wechseln, wann immer sie es für nötig halten, ohne dass dies größere Auswirkungen hat. Dies ermöglicht ihnen eine größere Flexibilität bei Entscheidungen über ihre IT-Infrastruktur und ihren Betrieb.

Umsetzung digitaler Souveränität bei Bare.ID

Mit Bare.ID erhalten Anwender die Vorteile einer erstklassigen Cloud Identity- und Access-Management-Lösung, die die deutschen Anforderungen an Datensicherheit und Datenschutz erfüllt. Bare.ID legt großen Wert auf die Einhaltung deutscher Gesetze und Vorschriften - von der Gerichtsbarkeit bis hin zum Support-Team, das in Deutschland ansässig ist, und den Rechenzentren, die sich in deutschen Unternehmen unter deutscher

Kontrolle befinden. Dies stellt sicher, dass alle Benutzerdaten mit den geltenden Vorschriften konform sind und bietet gleichzeitig eine zusätzliche Sicherheitsebene gegen potenzielle Bedrohungen oder Schwachstellen außerhalb der deutschen Grenzen. Außerdem achtet Bare.ID auch in der Lieferkette darauf, ausschließlich Lieferanten und Partner nach deutschen Sicherheitsstandards auszuwählen.

Um vollständig digitale Souveränität zu gewährleisten, bildet Bare.ID neben den rechtlichen und geografischen Anforderungen auch technologische Anforderungen bestmöglich ab. Im Kern der Lösung steht das etablierte Open Source IAM Framework Keycloak, welches eine einfache Datenportabilität gewährleistet. Sollte ein Anbieterwechsel gewünscht sein, besteht kein Vendor Lock-In und der Kunde kann seine Daten einfach zu einem anderen Anbieter mitnehmen. Alternativ kann er, durch den verfügbaren Source Code bei Bedarf auch ganz ohne Vendor arbeiten und ist somit völlig unabhängig.

Auch eine Ausfallsicherheit wird durch Hochverfügbarkeit garantiert, welche durch den Multi-Nodes Betrieb mit möglicher Georedundanz-Architektur gewährleistet wird: Mehrere Knoten werden verwendet, um Redundanz und Fehlertoleranz zu bieten, eine hohe Verfügbarkeit des Systems wird gewährleistet. Wenn ein Knoten ausfällt oder ein Problem auftritt, übernimmt ein anderer Knoten, um den Betrieb des Systems ohne Unterbrechung oder Datenverlust aufrecht zu erhalten. Darüber hinaus befindet sich mindestens zwei Knoten an einem anderen geografischen Standort entsprechend der KRITIS-Verordnung der Georedundanz.

Fazit

In der heutigen, sich ständig verändernden Technologielandschaft wird die digitale Souveränität für Unternehmen auf der ganzen Welt immer wichtiger. Um echte digitale Souveränität zu gewährleisten, muss also sicher sein, dass Mehrheitsanteile im deutschen Rechtsraum bleiben, Unternehmen die volle Kontrolle über ihre eigene IT-Umgebung behalten, gleichzeitig aber auch einen sicheren Zugriff mit hoher Verfügbarkeit bieten und die Abhängigkeiten an einzelne Anbieter vermeiden. Auf diese Weise sind sie in der Lage, eine echte Autonomie über ihre Daten zu bewahren und gleichzeitig die Vorteile von Cloud-Computing-Lösungen wie Skalierbarkeit und Kosteneinsparungen zu nutzen. Mit der richtigen Implementierung dieser Elemente können Unternehmen zuversichtlich in die Zukunft blicken - frei von unerwünschten Einschränkungen durch externe Anbieter oder Dritte.