VITAKO

HANDREICHUNG

Architekturbild Arbeitsplatz der Zukunft in der Verwaltung

Stand: 27. Februar 2024

INHALTSVERZEICHNIS

EINLEITUNG

Breit genutzte Standardanwendungen werden zunehmend in die Cloud verlagert. „On-Premises“-Lösungen, die auf Clients oder Servern der Anwender laufen, werden dagegen oft nicht mehr zur Verfügung gestellt. Private Unternehmen setzen bereits zu einem großen Anteil auf Cloud-Technologie, um ihre Daten zu speichern, zu verarbeiten und Prozesse effizienter und von überall verfügbar zu machen. Auch die öffentliche Verwaltung wird diesen Schritt gehen müssen, um die Vorteile der technologischen Entwicklung für sich nutzbar machen zu können, die benötigt werden, um den schwerwiegenden Herausforderungen, wie dem Fachkräftemangel oder der stetig ansteigenden Bedrohung durch Cyberangriffe, zu begegnen.

Derzeit werden in der Verwaltung aber zu einem großen Anteil noch Windows- und Office-Produkte der Firma Microsoft eingesetzt, die ebenfalls ab 2026 nur noch als Software as a Service (SaaS) angeboten werden sollen. Verschiedene Hyperscaler werben mit der Bereitstellung von „souveränen“ Cloud-Lösungen. Diese befinden sich teilweise noch in Entwicklung und es bleibt zu klären, ob sie die besonderen Anforderungen der öffentlichen Verwaltung erfüllen können. Daher müssen jetzt Alternativen der öffentlichen Hand entwickelt und die zahlreichen Fragen, die sich dabei stellen, beantwortet werden.

Ziel dieser Alternativen muss sein, der Verwaltung moderne Technologie zur Verfügung zu stellen und gleichzeitig deren digitale Souveränität und die der Bürgerinnen und Bürger zu wahren. Eine derartige Herausforderung kann nur in Kooperation der kommunalen, der Landes- und der Bundesverwaltungen gelingen. Wichtige Schritte auf diesem Weg sind die vom IT-Planungsrat beschlossene Deutsche Verwaltungscloud-Strategie[1] sowie das Projekt openDesk[2], bei dem verschiedene Stellen der öffentlichen Verwaltung und Open Source Hersteller kooperieren, um eine Open Source-basierte Arbeitsplatzumgebung zu entwickeln. Andere Verwaltungen auf kommunaler und Landesebene sowie IT-Dienstleister haben sich ebenfalls auf den Weg gemacht, verstärkt auf Open Source Alternativen zu setzen. An diese Bestrebungen möchte die vorliegende Handreichung anknüpfen und die Architektur eines souveränen Arbeitsplatzes der Zukunft in der öffentlichen Verwaltung skizzieren sowie Hinweise zu wichtigen Fragestellungen geben, die bei der Umsetzung geklärt werden müssen.

Damit ein solcher Arbeitsplatz die Anforderungen der digitalen Souveränität erfüllt und gemeinsam von vielen Akteuren für die öffentliche Verwaltung entwickelt werden kann, muss er soweit wie möglich auf Open Source Software (OSS) basieren. Der Wechsel zwischen Dienste-Anbietern wird erleichtert, offene Schnittstellen erlauben die Integration unterschiedlicher Systeme und die Überprüfbarkeit des Codes gewährleistet stets die volle Kontrolle über Anwendungen und Daten.

Der Erfolg eines Open Source Arbeitsplatzes wird in besonderem Maße auch von der Nutzerfreundlichkeit beeinflusst. Die Mitarbeiterinnen und Mitarbeiter werden den Schritt in neue Anwendungen und Umgebungen nur mitgehen, wenn ihnen im Vergleich zu den proprietären Programmen, in denen sie sich gute Kenntnisse angeeignet haben, deutliche Mehrwerte geboten werden. Der Wechsel zu einem Open Source System muss daher auch mit entsprechender Kommunikation begleitet werden. Nicht zuletzt spielen auch die Anforderungen der IT-Sicherheit eine wichtige Rolle.

---

[1] Vgl. https://www.cio.bund.de/Webs/CIO/DE/digitale-loesungen/digitale-souveraenitaet/deutsche-verwaltungscloud-strategie/deutsche-verwaltungscloud-strategie-node.html

[2] https://gitlab.opencode.de/bmi/opendesk/info

ÜBERGEORDNETE LEITLINIEN (NICHT-FUNKTIONALE ANFORDERUNGEN)

Der Arbeitsplatz der Zukunft ist digital souverän und hat Unabhängigkeit zum Ziel. Er ermöglicht die Wahlfreiheit zwischen unterschiedlichen Software-Produkten und die Kontrolle über die eigenen Daten.

- Der Arbeitsplatz der Zukunft basiert vor allem auf Open Source Software.
- Der Arbeitsplatz der Zukunft ist mobil.
- Der Arbeitsplatz der Zukunft bietet ein sicheres Arbeiten auf dem Stand der Technik.
- Für den Arbeitsplatz der Zukunft sind Kompatibilität und Interoperabilität notwendig.
    - Einheitliche Schnittstellen und Standards müssen beschrieben und in Ausschreibungen gefordert werden.
    - Integration von Fachverfahren: Hersteller müssen entsprechend offene Standards umsetzen, so dass Interoperabilität unabhängig von Basiskomponenten gegeben ist.
- Eine Community ist notwendig, um mit gebündelter Nachfrage („Marktmacht“) gegenüber Herstellern Feature-Requests zu stellen und um im Fall von Übernahmen eine Weiterentwicklung durch Bildung von Forks sicherzustellen.
- Eine Community der Fachverfahrenshersteller und öffentlichen IT-Dienstleister für die Weiterentwicklung von Fachverfahren wird benötigt. Die Koordination sollte durch das Zentrum für Digitale Souveränität erfolgen.
- Die Nutzerakzeptanz ist ein wesentlicher Faktor für den Erfolg des Arbeitsplatzes der Zukunft.
    - Interaktionsschnittstellen zwischen Nutzenden und Maschine entsprechen dem Stand der Technik.
    - Das System bietet für möglichst viele Nutzergruppen einen Mehrwert und hält Standards für Barrierefreiheit, Responsive Design und Usability ein.
    - Der Arbeitsplatz muss die wesentlichen Funktionen umfassen und die Bedienungsfreundlichkeit bieten, die Nutzerinnen und Nutzer von anderen Systemen gewohnt sind und erwarten.

ARCHITEKTURBILD

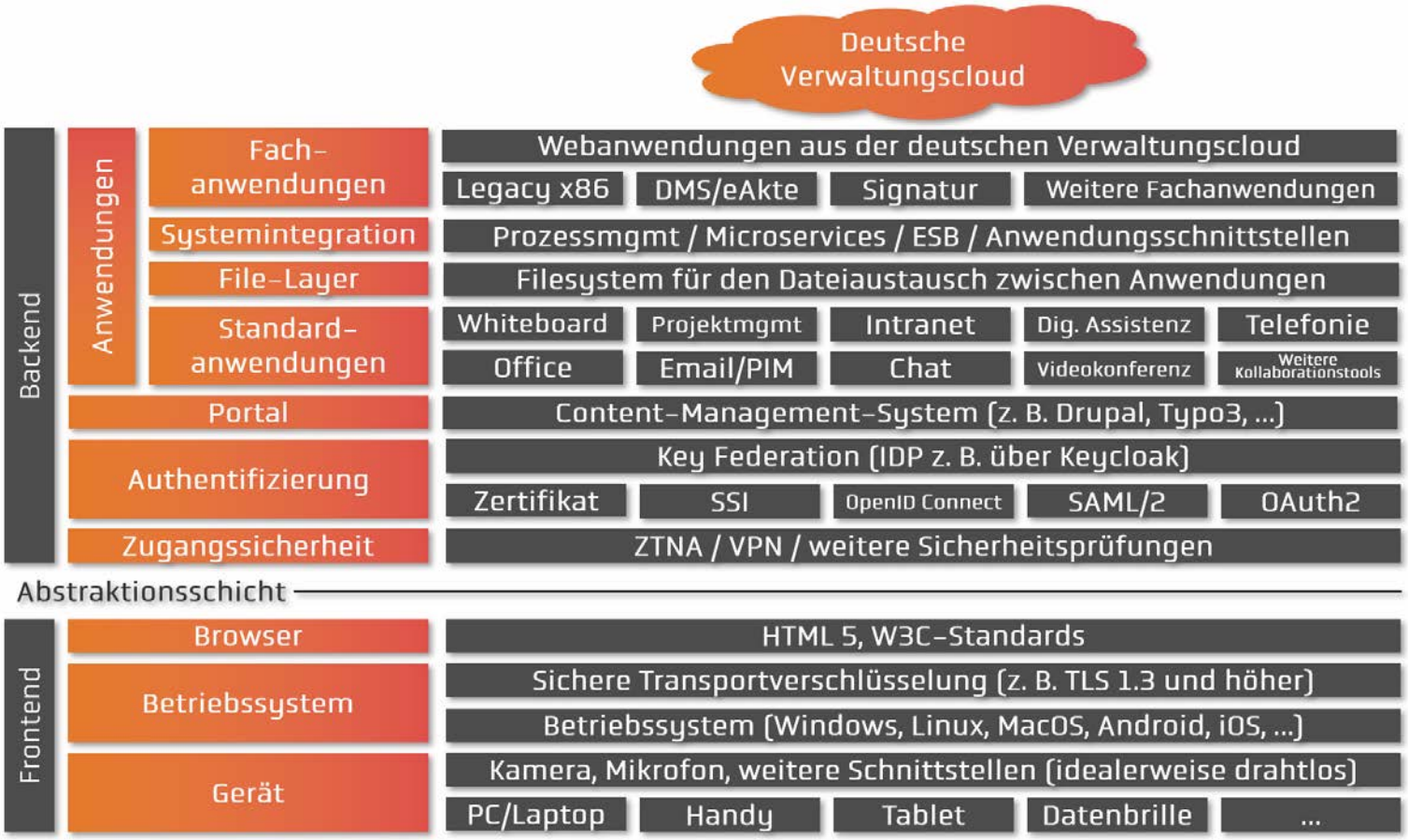

Abb. 1: Architekturbild Arbeitsplatz der Zukunft

FRONTEND

Durch die Nutzung eines Browsers als Abstraktionsschicht zwischen Frontend und Backend-Bereich kann eine weitgehende Unabhängigkeit von bestimmten Geräten oder Betriebssystemen erreicht werden. Somit können Nutzerinnen und Nutzer sowohl von einem PC oder Laptop als auch von Mobilgeräten auf ihre Anwendungen zugreifen. Auch in Zukunft genutzte Mensch-Maschine-Schnittstellen, wie z. B. Sprachassistenten oder Datenbrillen, können so bereits zu einem gewissen Grad antizipiert werden.

Die genutzten Geräte benötigen geeignete Schnittstellen für Kameras, Mikrofone oder andere Komponenten abhängig davon, was für die jeweilige Anwendung benötigt wird. Dabei ist zu beachten, dass die Sicherheitseinstellungen für den Zugriff von Anwendungen auf diese Schnittstellen auf die vorgesehenen bzw. zu erwartenden Nutzungsszenarien abgestimmt sind.

Auf dem Client können grundsätzlich alle üblichen Betriebssysteme eingesetzt werden, solange sie eine Form der Transportverschlüsselung, die dem gängigen Stand der Technik entspricht, unterstützen und die im Kapitel „Idealtypischer Standard für Client-Sicherheit“ beschriebenen Maßnahmen und Bedingungen ermöglichen.

Die Abstraktion durch den Browser sowie die Anforderungen daran werden im Kapitel „Abstraktion durch Webclient“ beschrieben.

BACKEND

Jeder Zugriff eines Clients auf die Infrastruktur und Anwendungen des Backends darf nur über einen abgesicherten Weg erfolgen. Idealerweise erfolgt der Zugriff auf die einzelnen Anwendungen nach dem Zero Trust Network Access Modell. Dabei erhalten Nutzende nur Zugriff auf die Anwendungen, für die sie berechtigt sind und müssen sich gegenüber diesen authentisieren. Wo noch keine Zero-Trust-Architektur implementiert ist, muss der Zugriff über eine VPN-Verbindung erfolgen. Beide Optionen ermöglichen jederzeit mobiles Arbeiten. Auf der Ebene der Authentifizierung stehen weitere Möglichkeiten der Absicherung zur Verfügung, wie der Austausch von Zertifikaten, die Nutzung einer Self Sovereign Identity sowie Authentifizierungsprotokolle, wie OAuth2, OpenID Connect und SAML 2.0. Lösungen auf dieser Basis müssen dann verbunden werden, um über eine zentrale Identitäts- und Zugriffsverwaltung die Authentifizierung über alle dahinterliegenden Anwendungen hinweg zu ermöglichen. Hier kann zum Beispiel Keycloak einen wichtigen Teil zur Lösung beitragen. Damit müssen Nutzerinnen und Nutzer sich nicht beim Aufruf einzelner Anwendungen immer wieder neu anmelden, sondern können fließend dazwischen wechseln. Gleichzeitig wird deutlich, dass durch ein bundeseinheitliches Identifikationssystem für die Verwaltung hier eine große Vereinfachung geschaffen werden könnte. Eine solche Verwaltungs-ID könnte z. B. auch in Verbindung mit der deutschen Verwaltungscloudstrategie flächendeckend umgesetzt werden.

Die Anwendungen selbst stehen über ein persönliches Portal zur Verfügung. Dieses bietet Nutzerinnen und Nutzern zunächst einen Überblick der Emails, Chatnachrichten und anderen wichtigen Meldungen in einem Dashboard. Über das Portal kann außerdem ein Intranet der Organisation abgebildet werden. Zusätzlich können auch IT-Dienste, wie ein Passwort Self Service, angeboten werden. Die wesentliche Funktion des Portals ist aber, Zugriff auf alle benötigten Basis- und Fachanwendungen zu bieten.

Zu den Basisanwendungen zählen zunächst die üblichen Office-Programme, wie Textverarbeitung und Tabellenkalkulation. Hinzu kommen Voice-over-IP-Telefonie, Email und Personal Information Manager (PIM), mit denen die persönlichen Kalender, Kontakte und Aufgaben verwaltet werden können. Videokonferenz- und Chat-Tools sowie ein virtuelles Whiteboard als zusätzliche Kommunikationsanwendungen ergänzt durch Projektmanagement-Tools werden benötigt, um kollaboratives und mobiles Arbeiten zu unterstützen. Darüber hinaus sollen auch digitale KI-Assistenten unter festgelegten Nutzungsbedingungen bei Bedarf eingebunden werden können.

Alle diese Anwendungen werden durch ein File-System als übergeordnete Schicht so integriert, dass Dateien direkt zwischen ihnen ausgetauscht werden können. Damit wird vermieden, dass diese die Betriebsplattform verlassen müssen, da sie nicht zunächst auf den Client heruntergeladen werden müssen, um dann wieder in eine andere Anwendung hochgeladen zu werden. Dazu müssen alle Anwendungen mit dem File-Layer verknüpft werden.

Im Hintergrund erfolgt eine weitere Integration aller Komponenten über Prozessmanagement-Tools, Service-Meshes, Enterprise-Service-Bus-Lösungen und Anwendungsschnittstellen. Damit sollen möglichst viele Anbindungen zwischen den einzelnen Anwendungen geschaffen werden, so dass Daten direkt zwischen ihnen ausgetauscht werden können.

Auf der darüber liegenden Ebene befinden sich schließlich die einzelnen Fachanwendungen der Verwaltung sowie eine Reihe von damit verbundenen Basisdiensten, wie e-Akte, ein Dokumentenmanagementsystem oder Dienste für elektronische Signaturen. Während das Ziel für Fachverfahren sein muss, dass diese zukünftig als Container bereitgestellt werden, muss zunächst zusätzlich auch ein Legacy-Bereich berücksichtigt werden, da bisher viele Verfahren auf den Betrieb als FAT-Client-Anwendung ausgelegt sind. Außerdem setzen sie oft Anbindungen an proprietäre Programme, wie z. B. Microsoft Office, voraus. Daher bleibt dieser Behelfsweg zunächst nötig, bis Fachverfahrenshersteller auch Schnittstellen zu Open Source Anwendungen für ihre Produkte bereitstellen.

Darüber hinaus muss der Arbeitsplatz der Zukunft auch Webanwendungen aus der Deutschen Verwaltungscloud einbinden können.

ABSTRAKTION DURCH WEB-CLIENT

Anstatt sich auf ein bestimmtes Betriebssystem festzulegen oder an unterschiedliche Betriebssysteme anpassen zu müssen, macht sich der Arbeitsplatz der Zukunft davon unabhängig. Dies gelingt durch den Rückgriff auf eine Abstraktionsschicht. Realisiert wird diese über einen Webbrowser, über den auf alle Anwendungen zugegriffen werden kann. Auf diese Weise erreicht man nicht nur eine Unabhängigkeit vom genutzten Betriebssystem, sondern auch in weiten Teilen von den eingesetzten Endgeräten. Die Nutzer können frei wählen, ob sie von einem Desktop-Rechner, Laptop oder mobilen Endgerät auf ihre Dateien und Anwendungen zugreifen, solange die Hardware die benötigte Leistungsfähigkeit erreicht.

Auch für den Betrieb von Anwendungen ergeben sich große Vorteile aus diesem Konzept. Software oder Updates müssen z. B. nicht mehr auf die vielen einzelnen Clients ausgerollt werden, sondern nur noch über die zentrale Infrastruktur bereitgestellt werden, wodurch erheblicher Aufwand eingespart wird.

Damit tatsächlich auf eine Vielzahl unterschiedlicher Anwendungen über einen Browser zugegriffen werden kann, müssen beide Seiten allerdings bestimmte Standards beherrschen. Ein wesentlicher Standard ist dabei HTML5. Besonders für die Kommunikation mit Webservices werden international anerkannte Standards benötigt, wie z. B. W3C-Standards, um auch die Kommunikation mit Cloud-Diensten zu ermöglichen. Darüber hinaus müssen zusätzlich Standards für Responsive Design, Barrierefreiheit und die Anbindung von Peripherie-Geräten eingehalten werden.

Ziel ist es, dass möglichst alle Browser, die die genannten Bedingungen erfüllen, genutzt werden können. Dennoch ist zu beachten: Derzeit zeigt sich am Angebot unterschiedlicher Webbrowser zumindest insoweit eine gewisse Konsolidierung, als dass viele davon inzwischen auf der gleichen Engine basieren. Um hier nicht wiederum in eine Abhängigkeit zu geraten, empfiehlt es sich, wenn möglich auf einen Open-Source-Browser zu setzen.

Damit dieses Konzept vollständig umgesetzt werden kann, müssen allerdings auch die Fachverfahren der Verwaltung darauf angepasst werden. Hier sind sowohl die privaten als auch die in öffentlicher Hand befindlichen Hersteller gefordert, diese entsprechend als Web-Anwendungen zur Verfügung zu stellen.

Beim Zugriff auf Anwendungen über den Browser muss auch ein Offline-Betrieb sichergestellt werden können, falls während des mobilen Arbeitens zeitweise keine Datenverbindung besteht. Dafür stehen zum Beispiel Technologien wie Progressive Web Apps und der WebAssembly-Standard (W3C) zur Verfügung.

ANWENDUNGEN

Alle Anwendungen müssen die Anforderungen der Deutschen Verwaltungscloud-Strategie erfüllen bzw. so gestaltet sein, dass sie auf einer Infrastruktur, die dem Konzept der Deutschen Verwaltungscloud-Strategie entspricht, betrieben werden können. Dabei muss außerdem die Portabilität zwischen verschiedenen Cloud-Umgebungen sichergestellt werden. Ziel für den Arbeitsplatz der Zukunft ist, dass alle Anwendungen als Container bereitgestellt werden können. Viele Softwareprodukte müssen dafür aber noch entsprechend angepasst werden. In diesem Zusammenhang ist es wichtig, dass von der öffentlichen Hand beauftragte Softwareentwicklungen stets als Open Source Software zur Verfügung gestellt werden.

Auf alle Anwendungen wird über den Browser zugegriffen. Die Anwendungen werden dann in einzelnen Tabs geöffnet. Wie bereits im Abschnitt Architekturbild beschrieben, müssen die einzelnen Anwendungen eng miteinander verknüpft werden. Mit entsprechenden Service Meshes ist dies sogar über Services aus unterschiedlichen Cloudumgebungen möglich. Z. B. kann so auf der Datei-Ebene vermieden werden, dass Dateien einen Umweg über den Client machen müssen. Außerdem müssen sie Daten mit anderen Komponenten austauschen können. Ein wichtiger Anwendungsfall ist die Authentifizierung. Nutzer sollen sich nur einmal anmelden müssen, um entsprechend ihren Berechtigungen Zugriff auf alle Anwendungen zu erhalten. Solche Integrationsmöglichkeiten zu schaffen, ist allerdings eine Herausforderung und hängt stark von der vorliegenden Architektur ab. Besteht diese aus Cloud-nativen Anwendungen, können bis zu einem gewissen Grad sogar Dienste über eine Hybridcloud- oder Multicloud-Umgebung hinweg mit einem entsprechenden Service-Mesh verbunden werden.

Um zu zeigen, dass es bereits für viele Anwendungsbereiche funktionierende Alternativen auf Open Source Basis gibt, soll die folgende Tabelle Beispiele für einige im Architekturbild genannte Komponenten geben, ohne dabei einen Anspruch auf Vollständigkeit zu erheben, da in diesem Rahmen keine umfassende Marktanalyse durchgeführt werden kann.

Anwendungsbereich	**Beispiele Open Source Produkte**
Zero Trust Network Access • Zugriffsverwaltung und IDP / IAM	Keycloak
VPN	Open VPN, WireGuard
Portal	Drupal, Wordpress, Typo3
Office	Collabora
E-Mail/PIM	Open Xchange
Chat	Rocket.Chat, Element
Videokonferenz	Jitsi, Big Blue Button, Element Call
Projektmanagement	OpenProject
Filesystem	Nextcloud, Owncloud
Wissensdatenbank	MediaWiki

Tab. 1: Beispiele für OSS in verschiedenen Anwendungsbereichen

IDEALTYPISCHER STANDARD FÜR CLIENT-SICHERHEIT

Um den Client angemessen absichern zu können, müssen eine Reihe von Voraussetzungen erfüllt werden, die hier als idealtypischer Standard zusammengefasst werden sollen.

Der Arbeitsplatz der Zukunft sollte möglichst auf einer Zero-Trust-Architektur aufgebaut sein und der Zugriff des Clients auf einzelne Anwendungen entsprechend nach den Prinzipien des Zero-Trust-Network-Access erfolgen. Wo eine solche Architektur noch nicht etabliert ist, sollten mindestens Maßnahmen nach dem IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik (BSI) ergriffen werden. In beiden Fällen ist eine Zertifizierung nach ISO 27001 bzw. IT-Grundschutz anzustreben. Zukünftig kann darüber hinaus auch eine Zertifizierung nach dem Kriterienkatalog C5[3] des BSI an Relevanz gewinnen.

Mit Blick auf den Client selbst ist es eine Grundvoraussetzung, dass dieser stets einen aktuellen Patch-Stand aufweist, was bedeutet, dass Geräten, für die keine Sicherheitsupdates mehr geliefert werden, kein weiterer Zugriff gewährt werden kann. Dies betrifft besonders das Betriebssystem, den Web-Browser und alle weiteren mit dem Internet verbundenen Applikationen. Im Fall von Managed Devices, die vollständig unter der Kontrolle der IT-Abteilung stehen, werden Updates zentral auf alle Clients ausgerollt. Vor allem sicherheitsrelevante Patches können so schnell verteilt werden.

Auf dem Client muss außerdem eine End Point Protection vorhanden sein. Dies kann bereits über die Sicherheitsfeatures des Betriebssystems abgedeckt sein oder muss anderenfalls über einen Anti Malware Dienst erfolgen.

Da der Zugriff auf Anwendungen vollständig über den Browser erfolgt, muss dieser entsprechend abgesichert werden. Um dies zu gewährleisten, muss der Mindeststandard für Web-Browser des BSI erfüllt werden[4].

Die Authentifizierung am Portal sowie am Gerät selbst erfolgt über mehrere Faktoren (Multi-Faktor-Authentifizierung). Damit dann der Zugriff auf die einzelnen Anwendungen problemlos funktioniert, müssen diese über ein entsprechendes Identitätsmanagement verfügen. Die Anmeldung am Portal muss über Verschlüsselung abgesichert werden: Zwischen Client und Portal muss eine TLS-verschlüsselte Verbindung bestehen. Der bei der Authentifizierung als Cookie im Browser abgelegte Token muss mit einer Session-Verschlüsselung gesichert sein.

Insgesamt ist für den Anmeldeprozess am Gerät und im Portal allerdings gleichzeitig darauf zu achten, eine gewisse Balance zwischen Sicherheit und Nutzerfreundlichkeit zu wahren, besonders im Hinblick auf den Einsatz von Multi-Faktor-Authentifizierung. Dies kann z. B. erreicht werden, indem der Einsatz mehrerer Faktoren abgestuft nach dem Sicherheitsniveau der Anwendung bzw. der Daten erfolgt.

Um zu gewährleisten, dass über den Arbeitsplatz der Zukunft auch Daten, die als VS-NfD eingestuft sind, verarbeitet werden dürfen, müssen entsprechende vom BSI dafür zugelassene Komponenten eingebunden werden können. Dafür müssen Schnittstellen in den betroffenen Anwendungen geschaffen werden, die eine Kompatibilität zu diesen Komponenten herstellen können.

---

[3] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/kriterienkatalog-c5_node.html

[4] Vgl. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_Sichere_Web-Browser_V2_0.html

Bei Unmanaged Devices, z. B. in der Form von Bring Your Own Device (BYOD), sind Nutzerinnen und Nutzer selbst in der Pflicht, Updates zeitnah durchzuführen. Sie müssen außerdem dafür sorgen, dass eine End Point Protection vorhanden und aktiv ist. Beides sollte möglichst durch eine Softwarekomponente auf dem Gerät laufend geprüft werden.

Sofern bei Unmanaged Devices Clientzertifikate eingesetzt werden und eine Identifikation über eine Self Sovereign Identity Lösung stattfindet, kann von einem hinreichenden Vertrauensniveau ausgegangen und der Zugriff auf alle Anwendungen ermöglicht werden. Ist dies nicht der Fall, muss für Unmanaged Devices eine Begrenzung der Zugriffsrechte festgelegt werden. Diese dürfen dann nur auf Anwendungen zugreifen, die keine Daten aus Sektoren kritischer Infrastrukturen, mit Schutzbedarf oder zu „Geschäftsgeheimnissen“ der Verwaltung verarbeiten.

NUTZERFREUNDLICHKEIT

Damit ein Verwaltungsarbeitsplatz auf Open Source Basis erfolgreich sein kann, müssen die Mitarbeiterinnen und Mitarbeiter in den Verwaltungen überzeugt werden. Der wesentliche Faktor dafür ist, dass die neuen Anwendungen möglichst intuitiv zu bedienen sind, über ein ansprechendes und übersichtliches Design verfügen, alle wichtigen Funktionen bieten und flüssig zu bedienen sind. Zusätzlich muss der Wechsel in eine neue Umgebung von entsprechender Kommunikation begleitet werden, sodass der Umstieg möglichst leichtfällt. Anderenfalls kann die Einführung von Open Source Software auch auf dieser Ebene scheitern. Bei der Personalgewinnung müssen ebenfalls die Vorteile kommuniziert werden, da die Verwaltung dringend benötigten Nachwuchs nur langfristig halten kann, wenn die aus dem Alltag bekannte Nutzerfreundlichkeit von Anwendungen auch in der Arbeitsumgebung gewährleistet ist.

Ebenso zentral sind die spezifischen Mehrwerte von Systemen aus quelloffenen Komponenten. Diese bestehen einerseits in der Souveränität über die verarbeiteten Daten, zu denen auch die Nutzungsdaten der Mitarbeiterinnen und Mitarbeiter gehören. Andererseits können über offene Schnittstellen einzelne Komponenten stark miteinander integriert werden und damit greifbare Vorteile bei Effizienz und Nutzerfreundlichkeit gegenüber proprietären Lösungen geschaffen werden. Dies wird von den Nutzenden erwartet und muss entsprechend umgesetzt werden.

Um die Verzahnung verschiedener Anwendungen vorantreiben zu können, ist gemeinschaftliche Arbeit der Verwaltungen, der IT-Dienstleister, der Open Source Hersteller und vielen anderen Akteuren der Community nötig, da der Aufwand allein viel zu groß wäre und Lösungen nicht immer wieder neu entwickelt werden müssen. Würde diese Praxis stärker im Markt verbreitet, könnte dies auch für die etablierten Hersteller ein Anreiz sein, offene Schnittstellen zu ihren Produkten bereitzustellen.