Linux-Arbeitsplatz für die öffentliche Verwaltung

SH

Schleswig-Holstein
Ministerium für Energiewende, Landwirtschaft, Umwelt, Natur und Digitalisierung

Schleswig-Holstein. Der echte Norden.

Inhalt

Ziele und Motivation

© Unsplash.com / Jud Mackrill

LINUX-STUDIE **ZIELE UND MOTIVATION**

Ziele und Motivation

Das zentrale IT-Management Schleswig-Holstein [ZIT SH] ist für **die Umsetzung der IT-Strategie der Landesregierung** in Schleswig-Holstein zuständig. In dieser Funktion hat das ZIT den IT-Dienstleister Dataport beauftragt, eine Machbarkeitsstudie [Analyse] für die Entwicklung eines alternativen Arbeitsplatzes für die Landesverwaltung Schleswig-Holstein, auf Basis des Open-Source-Betriebssystems GNU / Linux, durchzuführen.

Diese Analyse fand im Rahmen einer umfangreichen Untersuchung in den Jahren 2019 und 2020 statt. Im Ergebnis wurde das Vorhaben, einen **GNU** / Linux-Arbeitsplatz in Schleswig-Holsteins Landesverwaltung zu etablieren, als generell machbar bewertet. Die Ergebnisse wurden im Sommer 2020 dem ZIT präsentiert, woraufhin das ZIT Folgebeauftragungen auf den Weg gebracht hat, um auf die Zielvision eines Open-Source-entwickelten Linux-Arbeitsplatzes für die öffentliche Verwaltung in Schleswig-Holstein hinzuarbeiten.

Die Ergebnisse der durchgeführten Machbarkeitsstudie werden in diesem Dokument in Form einer Studie komprimiert dargestellt.
Die Marktdominanz von Microsoft im Segment der Betriebssysteme auf Verwaltungsarbeitsplätzen stellt ein Quasi-Monopol dar. Eine kritische Diskussion der Situation, im speziellen die Abhängigkeit von einem einzigen großen Hersteller in Bezug auf die digitale Souveränität der öffentlichen Verwaltung, ist daher sinnvoll und notwendig. GNU / Linux hat durch Hersteller:innen von Enterprise-Distributionen wie z. B. Red Hat, SUSE oder Canonical Ltd. den Sprung auf den Arbeitsplatz von Wirtschaftsunternehmen geschafft. Sind die Anforderungen eines Verwaltungsarbeitsplatzes etwa deutlich anders oder gar komplexer als in der Wirtschaft? Ist die Integration eines Linux-Arbeitsplatzes in eine Enterprise-Infrastruktur für Verwaltungen wirklich aufwendiger als dies in Wirtschaftsunternehmen der Fall ist? Oder bedarf es nur eines mutigen Versuches, das Thema groß zu denken und in kleinen Schritten gemeinsam anzupacken?

Hauptziel dieser Studie ist es, über Schleswig-Holstein hinaus Länder, Bundesbehörden und Kommunen zu ermutigen, einen öffentlichen Diskurs über den Einsatz von Linux auf Arbeitsplätzen der öffentlichen Verwaltung zu führen und Open-Source-Software [OSS] vermehrt für die Realisierung von IT-Projekten in Betracht zu ziehen.

GNU
ist ein Unix-ähnliches Betriebssystem, das vollständig aus freier Software besteht. GNU enthält selbst keinen Betriebssystem-Kern [Kernel], kann aber durch verschiedene Kernels ergänzt werden [meist: Linux, seltener: Hurd, FreeBSD].

LINUX-STUDIE **ZIELE UND MOTIVATION**

© Unsplash.com / 2h Media

© pexels.com / Fauxels

© Unsplash.com / Docusign

Des Weiteren werden **folgende Ziele** mit der Veröffentlichung dieser Studie verfolgt:

Weiterentwicklung auf Basis von Open Source

Die aktuelle Verwaltungsarbeitsplatz-Modellinie im Land Schleswig-Holstein basiert auf dem Betriebssystem Microsoft Windows 10. Für die Weiterentwicklung wurde beschlossen, die Landesverwaltungsarbeitsplätze in Schleswig-Holstein zukünftig auf Basis des Open-Source-Betriebssystems GNU/Linux zu betreiben.

Änderungen willkommen heißen [agiles Prinzip]

Im Rahmen der Weiterentwicklung werden bestehende Konzepte und Lösungen auf den Prüfstand gestellt. Nicht alle gewohnten Funktionen [z.B. Bedienkonzepte] werden sich 1:1 im neuen Produkt abbilden lassen. Es wird daher versucht, im Rahmen der ursprünglichen Anforderungen an einen Arbeitsplatz eine passende Lösung bereitzustellen.

Community-Management

Für eine gute und breite Zusammenarbeit mit Open-Source-Communitys wurde eine zentrale Anlaufstelle bei Dataport durch das ZIT beauftragt. Hier laufen ab sofort alle Aktivitäten gebündelt und zentral zusammen.
Sie erreichen das **Community-Management** unter:
community@melund.landsh.de.

Transparente Entwicklung und Mitarbeit

Die Weiterentwicklung des Produktes durch Dataport erfolgt transparent. Projektbegleitend wird es unterschiedliche Angebote zur Einsicht und Mitarbeit geben. Ansprechpartner ist das Community-Management.

Pionierarbeit

Das Bereitstellen eines von Anwender:innen akzeptierten Linux-Arbeitsplatzes mit vollem Funktionsumfang im Vergleich zu den kommerziellen Produkten am Markt wird in der Open-Source-Szene als „die Kür schlechthin" angesehen. Die durch Dataport für das ZIT erstellte Studie zur Machbarkeit stellt hier eine positive Gesamtbetrachtung dar. Das ZIT hat daher den IT-Dienstleister Dataport mit der Projektvorbereitung beauftragt.

Kooperationspartner:innen gesucht

Das ZIT SH ist interessiert an bundesweiten Kooperationspartner:innen, um die [Weiter-]Entwicklung eines generischen Linux-Arbeitsplatzes für die öffentliche Verwaltung gemeinsam voran zu treiben. Das Design des Arbeitsplatzes und seiner Managementumgebung soll nicht landesspezifisch erfolgen, sondern einen generischen Ansatz anbieten. Die Entwicklung wird vollständig quelloffen erfolgen, das Produkt wird in allen gängigen Behördentypen einsetzbar sein. Regional- oder behördenspezifische Anpassungen werden in das Produktdesign über definierte Schnittstellen integrierbar sein.

Open-Source-Strategie

2

Open-Source-Strategie

Die zunehmende Digitalisierung ändert die Arbeitsweise der Öffentlichen Verwaltung. Auch **die Rahmenbedingungen ändern sich**. So werden Daten zu einem begehrten Gut und Anbieter:innen proprietärer Software gehen dazu über, Leistungen nur in Verbindung mit Betriebs- und Rechenzentrumsleistungen anzubieten.

Vor diesem Hintergrund muss geprüft werden, wie die digitale Souveränität erhalten werden kann. **Digitale Souveränität bezeichnet „die Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle[n] in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können und damit die Übertragung des Prinzips der ‚Selbstbestimmung' ins digitale Zeitalter"**[1]. Die Umstellung auf Open-Source-Lösungen ist dafür ein wesentlicher Baustein. Die transparente Entwicklung eines mobilen Linux-Arbeitsplatzes trägt für mehr digitale Souveränität in der Landesverwaltung Schleswig-Holstein bei.

[1] Vgl. Schleswig-Holstein Landesregierung 2020, S. 5.

LINUX-STUDIE **OPEN-SOURCE-STRATEGIE**

Dataport als **Open-Source-IT-Dienstleister**

Dataport Anstalt des öffentlichen Rechts [AöR] ist der IT-Dienstleister aus dem Norden für die öffentliche Verwaltung. Gemeinsam mit Ländern und Kommunen gestaltet Dataport den digitalen Wandel. Als Partner in allen Digitalisierungsvorhaben begleitet Dataport den öffentlichen Sektor, von der ersten Idee bis hin zum sicheren Betrieb. Dafür kooperiert Dataport mit Anbieter:innen aus der Region und unterstützt die föderale IT-Kooperation. Als AöR wird Dataport von den Ländern Bremen, Hamburg, Mecklenburg-Vorpommern, Niedersachsen, Sachsen-Anhalt und Schleswig-Holstein sowie dem kommunalen „IT-Verbund Schleswig-Holstein" getragen. Dataport hat ca. 4.000 Mitarbeiter:innen und erzielte 2021 einen Umsatz von etwas über einer Milliarde Euro.

Dataport verfolgt eine Stärkung der digitalen Souveränität seiner Kund:innen und Eigentümer:innen. Dies ist sowohl in der Hybrid-Strategie als auch der Multi-Vendor-Strategie verankert. Die Nutzung von Open Source ist ein wesentlicher Bestandteil beider Strategien. Mit der Hybrid-Strategie werden parallel zwei Wege beschritten, um eine Unabhängigkeit von den großen, marktbeherrschenden, vor allem US-amerikanischen Unternehmen zu erreichen. Erstens besteht sie aus Verhandlungen, um die bisher verwendeten Produkte On-Premises nutzen zu können. Zweitens ist die Etablierung von Alternativen zu derzeit genutzter Software zu entwickeln. Hierzu zählen insbesondere Open-Source-Produkte. Die Multi-Vendor-Strategie zielt darauf ab, Abhängigkeiten wirtschaftlicher und technologischer Art von einzelnen Partner:innen zu vermeiden. Durch eine Diversifizierung kann u.a. die Sicherheit und Stabilität besser gewährleistet werden, da im Fall von kompromittierten Systemen andere funktionsfähig bleiben und den Betrieb aufrechterhalten. Deswegen wird auf unterschiedliche Anbieter:innen gesetzt. Dazu gehören insbesondere Open-Source-Produkte.

Dataport nutzt bereits in vielfältiger Weise Open-Source-Lösungen, z.B. in den Bereichen Server und Datenbanken. In jedem Einzelfall wurden Wirtschaftlichkeit, Stabilität, Abhängigkeit von Hersteller:innen und Zukunftsfähigkeit geprüft. Dataport sieht sich verpflichtet, sich strategisch und praktisch noch intensiver mit Open Source zu befassen. Dafür sollen eine Open-Source-Geschäftsstrategie entwickelt und die Entwicklung eigener Open-Source-Lösungen intensiviert werden. Außerdem baut Dataport die Partnerschaften im Bereich der öffentlichen IT-Dienstleister:innen auf Bundes-, Landes- und Kommunalebene aus. Dataport intensiviert zudem die Kooperationen mit der Open-Source-Community und präzisiert die eigene Rolle. Denn die Kooperation wird nur gelingen, wenn Dataport sich aktiv in die Community einbringt.

Fortsetzung ▸

Einsatz und Entwicklung von Open Source in Schleswig-Holstein

Durch den Koalitionsbeschluss der aktuellen Landesregierung in Schleswig-Holstein wurde eine vermehrte Nutzung quelloffener Software vereinbart. Das langfristige Ziel ist eine vollständige Ablösung.[2] Gleichzeitig ist Schleswig-Holstein an Initiativen im Rahmen eines nationalen Aktionsplanes für offenes Verwaltungshandeln beteiligt. Das heißt, es besteht das klare politische Bekenntnis, sich vermehrt einem quelloffenen System zuzuwenden. In einem Landtagsbeschluss von 2018 wurde weiter festgelegt, dass bei wesentlichen Änderungen oder Neuvergabe möglichst viele Verfahren auf Open-Source-Software umgestellt werden sollen. **Neben der Funktionalität sind dabei auch Sicherheit, Wirtschaftlichkeit, Bedienbarkeit und Interoperabilität wesentliche Zielgrößen.**[3] **Dies wurde im März 2020 weiter fixiert.**[4] Auf diese Weise wird die Abhängigkeit der öffentlichen Verwaltung von einzelnen Softwareanbieter:innen so weit wie möglich reduziert. Zudem wird die Souveränität der Verbraucher:innen verbessert, die IT-Sicherheit erhöht und innovative Anwendungen werden ermöglicht. Auch unter dem Aspekt Green-IT stellt Open-Source-Software [OSS] einen wesentlichen Vorteil gegenüber proprietärer Software dar. Denn durch quelloffene Software wird ersichtlich, wie ressourceneffizient die Software gestaltet ist.

Seitens des Zentralen IT-Managements Schleswig-Holstein [ZIT SH] wurde und wird das Thema „Einsatz von Open-Source" – in Zusammenarbeit mit den Ressorts der Landesverwaltung, Dataport und dem Verbund der Träger:innen Dataports – bereits seit mehreren Jahren vorangetrieben, sodass Schleswig-Holstein in Sachen Einsatz von Open Source bereits gut aufgestellt und vernetzt ist. Open Source ist u.a. in den Rechenzentren und einzelnen Komponenten am Arbeitsplatz im Einsatz. Zukünftig soll im Kontext der Softwareentwicklung das Ziel einer quelloffenen Entwicklung verfolgt werden. Ein weiterer Schritt ist die Freigabe von Entwicklungsergebnissen des Landes unter freien Lizenzen. Da die Standardarbeitsplätze des Landes noch überwiegend mit proprietärer Software ausgestattet sind, werden sich die zukünftigen Anstrengungen auf diesen Bereich fokussieren. **Bis Mitte 2022 soll der Einsatz von Linux zur Ablösung von Microsoft Windows erprobt worden sein.**[5]

Mit der Einführung eines Standardarbeitsplatzes stellte das Land Schleswig-Holstein eine einheitliche Infrastruktur in der gesamten Landes- und Kommunalverwaltung auf der Ebene der Bürokommunikation und der Bereitstellung gemeinsamer zentraler Dienste zur Verfügung. Datenschutzrechtlichen Anforderungen und den aktuellen Standards für IT-Sicherheit kommen bei dem Arbeitsplatz besonderes Gewicht zu. Der aktuelle Standardarbeitsplatz enthält Softwarekomponenten, die teilweise aufeinander aufbauen. So bildet Windows 10 als Betriebssystem die Basis für weitere Software wie z.B. die Bürokommunikationssoftware. Der zukünftige Open-Source-basierte Arbeitsplatz muss dementsprechend auf einem modularen System basieren, für das plattformübergreifend Standardanwendungen enthalten sind. So wird z.B. bis Ende 2024 der überwiegende Teil der IT-Arbeitsplätze in Schleswig-Holstein mit **LibreOffice** ausgestattet sein. Die Installation löst das Produkt Microsoft Office ab. Auch die Fachverfahrenslandschaft muss gleichzeitig einen Wandel durchlaufen: Anwendungen müssen in einer plattformunabhängigen Fachverfahrenslandschaft bereitgestellt werden und unabhängig vom Betriebssystem des Arbeitsplatzes nutzbar sein. Perspektivisch soll ebenfalls das Microsoft Active Directory in Schleswig-Holstein durch eine Open-Source-Lösung abgelöst werden.

Quellen

[2] Vgl. CDU, Grüne, FDP 2017, S. 108

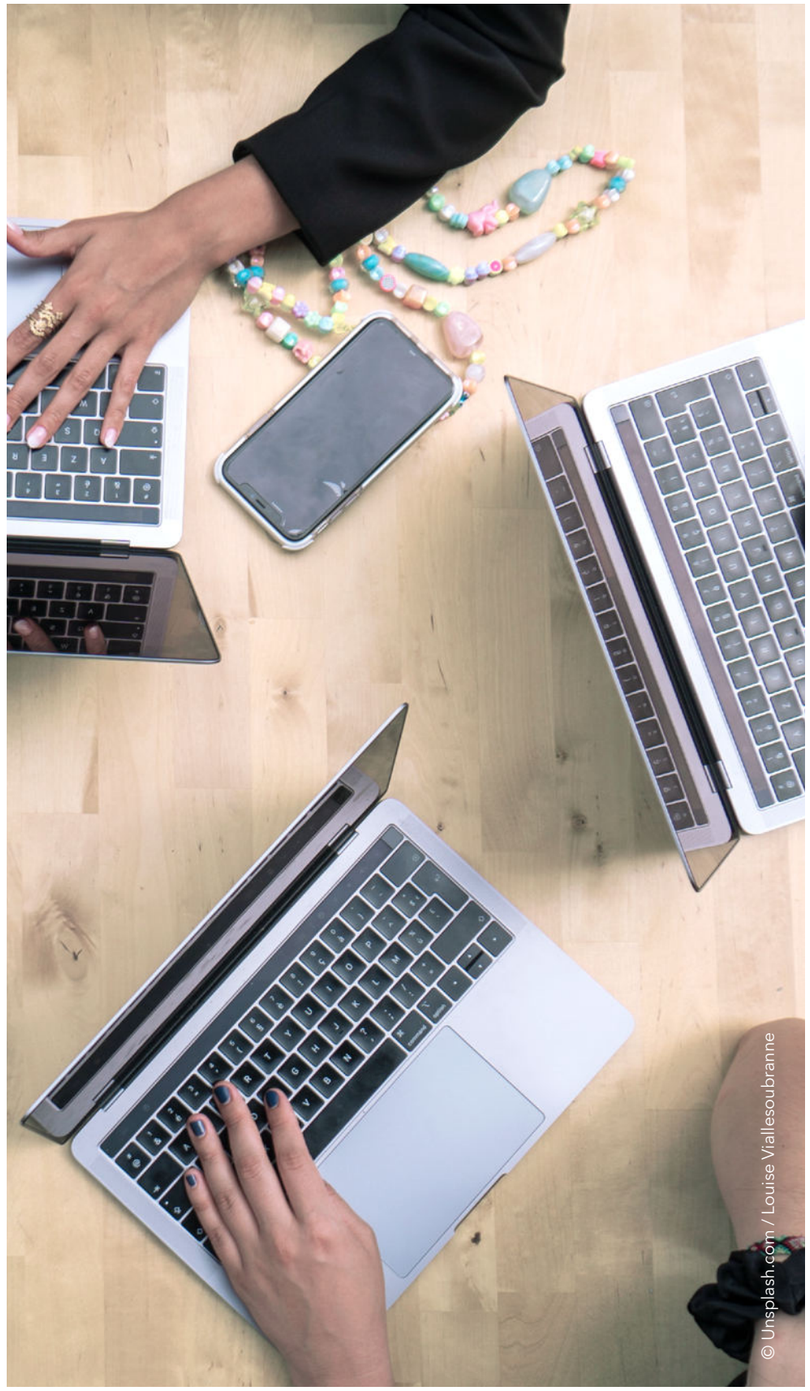
[3] Vgl. Schleswig-Holsteinischer Landtag 2018

[4] Vgl. Schleswig-Holstein Landesregierung 2020

[5] Vgl. Schleswig-Holstein Landesregierung 2020

LibreOffice
ist ein freies und quelloffenes Office-Paket, das verschiedene Anwendungen vereint. Dazu zählen Werkzeuge zur Textverarbeitung, Tabellenkalkulation, zur Datenbankverwaltung, ein Präsentationsprogramm, ein Zeichenprogramm und ein Formeleditor **www.libreoffice.org.**

LINUX-STUDIE **OPEN-SOURCE-STRATEGIE**


© Unsplash.com / Louise Viallesoubranne

OPEN-SOURCE-SOFTWARE

Wir verwenden die Bezeichnung Open-Source-Software, verstehen darunter aber freie und Open-Source-Software. Der Begriff „freie Software" bezieht sich in seinem Ursprung nicht auf „kostenlose" Software, sondern auf bestimmte Freiheiten bei der Verwendung von Software. Diese Freiheiten sind meist erweiterte Rechte der Nutzung, die u.a. den freien, unentgeltlichen Zugang zur Software, deren Änderung und uneingeschränkte Weitergabe erlauben – auch zu kommerziellen Zwecken.

Um diese Freiheiten in Anspruch nehmen zu können, muss der Quellcode von Software zwangsweise offen zugänglich sein. Freie Software ist somit auch immer quelloffen, also Open-Source. Eine Definition von Open-Source-Software wird von der international anerkannten Open-Source-Initiative [opensource.org] gegeben, die Open-Source-Lizenzbedingungen anhand von 10 Kriterien einstuft und auf Antrag zertifiziert.

Anforderungen

3

Anforderungen

Der erste Schritt im Design eines Arbeitsplatzproduktes ist die Definition von Anforderungen. Durch die verschriftlichte Ausarbeitung von Anforderungen ist es möglich, den gewünschten Zielarbeitsplatz zu beschreiben. Dies bildet die Arbeitsgrundlage, aus der später ein standardisiertes Produkt entsteht.

In diesem Zusammenhang spricht man auch von einer „Arbeitsplatz-Modelllinie". Eine Modelllinie umfasst neben dem Arbeitsplatzprodukt auch die notwendige Infrastruktur, die für die Nutzung, Verwaltung und den Betrieb der Arbeitsplätze benötigt wird. Das Konzept für Modelllinien wird verwendet, um standardisierte Arbeitsplatzprodukte in unterschiedlichen Verwaltungen auf einer gemeinsamen Basis anzubieten. Durch den hohen Grad an Standardisierung entsteht für den:die Kund:in [z. B. öffentliche Verwaltungen] und dem:die Anbieter:in [IT-Dienstleister:in] ein Mehrwert, der sich sowohl in einer hohen Qualität, aber auch in passenden Kostenmodellen ausprägt.

Anforderungen an einen Verwaltungsarbeitsplatz

Grundsätzlich ist ein Verwaltungsarbeitsplatz vergleichbar mit einem modernen, ggf. mobilen Büroarbeitsplatz. Durch das vielfältige Aufgabenspektrum der öffentlichen Verwaltung wird jeder Arbeitsplatz im Normalfall durch Fachanwendungen ergänzt. Als Fachanwendung oder Fachverfahren wird Individualsoftware bezeichnet, die für jeweils einen bestimmten fachspezifischen Verwaltungsaufgabenprozess bzw. Aufgabenbereich erstellt wurde.

Anforderungen
an einen Arbeitsplatz für Bürokommunikation

Entscheidend für den Erfolg eines Arbeitsplatzes ist die Akzeptanz seitens der Anwender:innen. Daher steht ein anwenderfreundliches Design immer im Mittelpunkt der Entwicklung neuer Arbeitsplatz-Modelllinien, um eine bestmögliche intuitive und einfache Bedienbarkeit sicherzustellen. Auch ein barrierefreies Design muss frühestmöglich im Designprozess berücksichtigt werden.

Ein standardisierter Arbeitsplatz zeichnet sich neben dem Erscheinungsbild auch durch seine abgestimmte Software aus. Durch eine gute Vorauswahl der Basissoftware und optimierte Vorkonfigurationen wird ein optimal nutzbarer Arbeitsplatz geschaffen. Je nach Einsatzzweck wird dieser durch Fachverfahren ergänzt.

Beispiele für Basissoftware auf einem Verwaltungsarbeitsplatz:

- **Office-Software**
  Textverarbeitung, Tabellenkalkulation, Präsentationen, …
- **Groupware**
  Kalender, Kontakte, Aufgaben, Termine, Raumbuchung, …
- **Kommunikationssoftware**
  E-Mail, Chat, Audio-/Videotelefonie und -konferenz, …
- **Sicherheit**
  Passwortverwaltung, Virenscanner, Dateiverschlüsselung, …
- **Hilfsanwendungen**
  Taschenrechner, PDF-Betrachter, Packprogramm, …
- **Multimedia**
  Audio-/Video-Player und Recorder, Bildbearbeitung, …
- **Barrierefreiheit**
  Leselupe, Sprachsteuerung, Live-Untertitelung, …
- **Dokumentenverwaltung**
  digitale Aktenhaltung, …

Sicherheitsanforderungen
an einen Verwaltungsarbeitsplatz

Die Sicherheit von Daten spielt eine elementare Rolle bei Arbeitsplätzen in der öffentlichen Verwaltung. Bereits bei der Auswahl der Endgeräte werden daher grundlegende Anforderungen an deren Sicherheitsfunktionen gestellt. Durch spezielle Chip-Sätze in den Endgeräten werden Funktionen wie gesichertes Starten des Betriebssystems und das automatische Entschlüsseln von verschlüsselten Datenträgern ermöglicht. Optional können Datenträger über

Fortsetzung ▸

Die Sicherheit von Daten ist eine der Grundanforderungen beim Design eines souveränen Verwaltungsarbeitsplatzes.

Trusted-Platform-Module
Ein Micro-Controller in modernen Computern, der [Speicher-]Hardware vor Missbrauch auf Basis integrierter Kryptografieschlüssel schützt.

Mehrfaktorverfahren stärker abgesichert werden [z. B. Entschlüsselung des Datenträgers nur in Kombination von TPM-Chip und zusätzlichem USB-Token, welches beim Starten des Systems an das Endgerät angeschlossen sein muss].

Für das Betriebssystem legen Richtlinien standardisierte Sicherheitseinstellungen auf Ebene des Systems und der Benutzer:innen fest. Diese lassen sich durch Anwender:innen nicht umgehen und werden über die Systemadministration der Arbeitsplätze gepflegt und gesteuert. Durch Rollenmodelle für Benutzer:innen und Gruppen werden Rechtebeschränkungen für Anwendungen und die Rechtevergabe auf Dateisystemebene [Dateien und Verzeichnisse] abgebildet.

Eine weitere, wichtige Anforderung, die in den letzten Jahren verstärkt an Bedeutung gewonnen hat, sind Einschränkungen bei der Übermittlung von Benutzer:innen-, Geräte- und Lizenzinformationen an Hersteller:innen. Diese sind auf ein notwendiges Minimum einzugrenzen.

Offline-Fähigkeit des Endgeräts und mobiles Arbeiten

Eine wichtige Anforderung an die Linux-Arbeitsplatz-Modelllinie ist ein grundlegendes Maß an Robustheit bzgl. der verschiedenen Möglichkeiten, mit dem Internet verbunden bzw. nicht verbunden zu sein. Netzwerkwechsel und die damit einhergehenden Funktionen und Funktionseinschränkungen zwischen Behördennetz, unbekannten Netzwerken [Hotspot-WiFi, o. Ä.] oder dem Homeoffice müssen sich den Anwender:innen transparent erschließen.

Es muss möglich sein, grundsätzlich produktiv weiterzuarbeiten, unabhängig von der Konnektivität des Endgeräts. Kurze Offline-Phasen sollten das produktive Arbeiten nicht beeinträchtigen, für längere Offline-Arbeitsphasen muss es möglich sein, diese vorzubereiten. Alle diese Vorgänge müssen ohne administrative Rechte auf dem Endgerät für Anwender:innen nutz- und bedienbar sein bzw. ohne Eingriff des:der Benutzer:in automatisch im Hintergrund stattfinden.

Insbesondere für systemnahe Funktionen sind für die Linux-Arbeitsplatz-Modelllinie Konzepte für Offline-Fähigkeit zu entwickeln und zu implementieren. Hierzu gehören:

- **Anmeldeverfahren**
- **Synchronisation von Speicherorten**
  - Persönliche Dateien der Anwender:innen
  - Daten auf Netzlaufwerken und Gruppenablagen
  - Daten in On-Premises-Cloud-Lösungen
- **Benutzer:innenprofile**
  z. B. Profil-Roaming

Langfristig sollen auch kollaborative Funktionen bei der Arbeit mit dem Linux-Desktop mit grundlegenden Offline-Fähigkeiten ausgestattet werden:

- **Mail**
  Lesen bereits erhaltener Mails, Verfassen neuer Mails
- **Groupware**
  Kontakte, Kalender etc.

Anforderungen an **Enterprise-Umgebungen** [Infrastruktur]

Das Ziel von Enterprise-Infrastrukturen ist die Bereitstellung von passenden und unterstützenden Diensten für die Arbeitsplätze in einem optimalen Kosten-/Leistungsverhältnis für den:die Kund:in und den:die IT-Dienstleister:in.

Enterprise-Umgebungen werden dabei mit hohem Qualitätsanspruch an Performance, Skalierbarkeit und Verfügbarkeit entworfen und betrieben. Vorgaben bzgl. IT-Sicherheit und Datenschutz [z. B. durch das BSI] geben hierfür den Rahmen vor.
Aus Sicht eines:einer IT-Dienstleister:in wird dieser Anspruch ergänzt – um die Themenbereiche der zentralen Verwaltung [operatives Management], einer optimalen Automatisierung im Betrieb und einer Lösung für die Unterstützung der Anwender:in [Fernwartung].

Anforderungen an **zentrale Dienste**

Wie bereits erwähnt, erfolgt die Entwicklung eines standardisierten Arbeitsplatzes in der Regel in Form von Modelllinien. Durch grundlegende Designs werden mandant:innenfähige Betriebsmodelle entwickelt, um eine sichere Trennung

Fortsetzung ▸


© pexels.com / This is engineering

der IT-Infrastruktur der verschiedenen Kund:innen abzubilden. Verteilte Infrastrukturelemente sind durch die unterschiedlichen Standorte der Verwaltungen der Normalfall. Durch einheitliche Lösungsdesigns werden eine standardisierte Nutzung, aber auch ein optimaler und wirtschaftlicher Betrieb möglich.

Sowie die Verwaltung der Arbeitsplätze erfolgt auch die Administration der genutzten Dienste [Infrastruktur] auf Basis von zentralen Betriebsmodellen. Dabei steht stets die Automatisierung von Prozessen, z.B. die Bereitstellung oder Außerbetriebnahme von Arbeitsplätzen, im Fokus. Auch die Softwareverwaltung inklusive einer Mandant:innentrennung [Kund:innen] wird z.B. durch Konzepte wie Softwarewarenkörbe [Self-Service] standardisiert und somit effektiv auf dem Endgerät nutzbar gemacht. [Field-]Service und Anwender:innen-Support erfolgen über klar geregelte Schnittstellen und sind optimal mit den Prozessen [IT-Servicemanagement] des:der IT-Dienstleister:in abgestimmt.

Automatisierung von Betriebsprozessen ist die Grundlage für die Entwicklung von mandant:innenfähige Modelllinien.

Die Weiterentwicklung der Modelllinien erfolgt über Produktreleases [Versionen] und ermöglicht dem:der Kund:in so eine Planungsgrundlage, um seine:ihre IT-Landschaft trotz ggf. zeitlicher Einschränkungen fortzuschreiben.

Das grundlegende Design aller Dienste bzw. der notwendigen Infrastruktur erfolgt immer unter Berücksichtigung von Aspekten des Datenschutzes und der IT-Sicherheit. Die Standardisierung stellt dabei den notwendigen Rahmen zur Verfügung, durch den ein professioneller Betrieb ermöglicht wird. Sämtliche Maßnahmen z.B. gesteuertes Firmware-, und Kernel-Updatemanagement sowie die Bereitstellung von Funktions- und Sicherheitsupdates für Softwarepakete stellen die ganzheitliche Pflege der Infrastruktur sicher.

Beispiele für zentrale Dienste [Infrastrukturen]:

- **Identitätsverwaltung**
  Dienstübergreifende Nutzung und Verwaltung der Benutzer:innen, Gruppen und Ressourcenzuordnungen
- **VPN**
  Einwahl in den Netzwerkbereich der Verwaltung
- **Drucker**
  Nutzung der Druckerpools vor Ort in den Standorten
- **Systemmanagement**
  Firmware-, Treiber-, Update- und Patch-Management
- **E-Mail**
  Nutzung des zentralen E-Mail-Dienstes
- **Benutzerdatenhaltung**
  Exklusive Dateiablagestruktur für Anwender:innen
- **Laufwerke für Datenhaltung**
  Datenaustausch, Gruppen- oder Projektlaufwerke

Multi-Vendor-Strategie der neuen Modelllinie

Eine wichtige Anforderung an das Gesamtkonzept der Linux-Arbeitsplatz-Modelllinie, und insbesondere der zugehörigen Infrastruktur, ist das Auflösen der verschiedenen Abhängigkeiten von einzelnen Hersteller:innen. Durch den Einsatz von Open-Source-Software wird es deutlich einfacher sein als bisher, bei der Konzipierung der Modelllinie die neue Anforderung einer Multi-Vendor-Strategie im Land Schleswig-Holstein auf technischer und organisatorischer Ebene zu implementieren.

IM KONTEXT MULTI-VENDOR WERDEN VERMEHRT COMMUNITYS, DISTRIBUTOR:INNEN UND ENTERPRISE-PARTNER:INNEN AN DIE STELLE EINZELNER HERSTELLER RÜCKEN.

Allgemein ist in den meisten Fällen der Einsatz einer freien und Open-Source-Software [OSS] möglich, ohne eine Geschäftsbeziehung mit dem:der Hersteller:in der genutzten Software eingehen zu müssen. Grundsätzlich löst sich durch den Einsatz von Open Source in vielen Bereichen der IT-Landschaft der Begriff des:der Hersteller:in auf. An dessen:deren Stelle rücken Begriffe wie „Distributor:innen", „OSS-Communitys" und „Enterprise-Support-Partner:in". Für eine verlässliche Enterprise-IT sind weiterhin vertraglich abgesicherte Partnerschaften mit Unternehmen, die Enterprise-Support anbieten, für die meisten Softwareprodukte unumgänglich.

Die verschiedenen Open-Source-Communitys bieten in vielen für den Linux-Arbeitsplatz [und dessen Infrastruktur] relevanten Bereichen eine Vielfalt an hochwertigen Produktlösungen, die in ihrer Funktion gleichwertig und somit teilweise gegeneinander austauschbar sind. Die meisten dieser Produkte sind auf Interoperabilität mit anderen OSS-Produkten ausgelegt und bieten Unterstützung für mehrere Linux-Distributionen. Dies gilt insbesondere für den Bereich des Systemmanagements [**vgl. S. 54**]. Auch bzgl. der Linux-Distribution selbst [**vgl. S. 74**] hat sich gezeigt, dass es für den Linux-Arbeitsplatz mehrere Optionen gibt [d.h. mehrere Distributionen kommen potenziell als Arbeitsplatz-Betriebssystem infrage].

Grundsätzlich ergibt sich aus der Anforderung nach Handeln auf Basis einer Multi-Vendor-Strategie implizit eine Anforderung an die Organisation der Projektvergabe für Enterprise-Support. Um bzgl. der zum Einsatz kommenden Produkte langfristig nachhaltig und flexibel aufgestellt zu sein, wird es für den Aufbau und Support der allgemeinen Systemkomponenten [d.h. insbesondere Linux-Distribution und Systemmanagement] sinnvoll sein, auf IT-Generalisten zu setzen. In bisherigen Lösungen wurde ein Produkt gewählt und dann bei dem:der Hersteller:in Enterprise-Support dafür eingekauft. Open Source macht es möglich, den Enterprise-Support eines:einer Hersteller:in einer kostenpflichtigen Software mit dem Support von Linux-Expert:innen zu kombinieren, die unabhängig von den Hersteller:innen sind. Da die Linux-Arbeitsplatz-Modelllinie mittelfristig zunächst gegen eine Windows-Infrastruktur [insbesondere IAM] betrieben werden soll [**vgl. S. 58**],

Fortsetzung ▸

ist Mischexpertise [Linux/Windows] bei externen und internen Fachkräften eine wichtige Zusatzanforderung.

Um der Anforderung einer Multi-Vendor-Strategie auf technischer Ebene gerecht zu werden, wird es wichtig sein, gleich zu Beginn die Schnittstellen zwischen den verschiedenen Softwarekomponenten vom Arbeitsplatz und seiner Enterprise-Infrastruktur möglichst generisch zu konzipieren. Harte Abhängigkeiten, insbesondere zwischen Arbeitsplatz und Infrastruktur, gilt es von Beginn des Produktdesigns an zu vermeiden.

Konkret bedeutet dies für die Linux-Arbeitsplatz-Modelllinie, dass bei der Entwicklung der Modelllinie bzgl. verschiedener Komponenten [Softwareprodukte] immer „mehrgleisig gedacht" werden muss.

Gibt es für ein technisches Detail mehrere Lösungsansätze, sind die entsprechenden Komponenten der neuen Arbeitsplatz-Modelllinie möglichst produktneutral zu entwickeln.

Beispiele für Komponenten der Linux-Arbeitsplatz-Modelllinie, die langfristig austauschbar bleiben sollten:

- **GNU-/Linux-Distribution**
- **Desktop-Umgebung**
  Software der Arbeitsoberfläche
- **Standardwebbrowser**
- **Life-Cycle-Management Frontend**

Prozesse für die Arbeitsplatzverwaltung

Die Verwaltung von Arbeitsplatz-Modelllinien eines:einer IT-Dienstleister:in erfolgt über definierte und aktiv gemanagte Prozesse.

Beispielprozesse für die Verwaltung einer Enterprise-Modelllinie:

Auftragssteuerung
Die Auftragssteuerung ist für den:die Kund:in der zentrale Eingangskanal, um die Arbeitsplätze im eigenen Haus zu verwalten. Über diesen Prozess ist es möglich, die Inbetriebnahme und Außerbetriebnahme oder Umzüge von Anwender:innen zu beauftragen.
Auch die Installation und Deinstallation von Software auf Arbeitsplätzen, die nicht dem Modelllinien-Standard entspricht, wird an dieser Stelle beauftragt [außer: Self-Service-Software-Warenkörbe].

Standardersatzbedarf
Regeltausch von Endgeräten
Austausch von Arbeitsplätzen im Rahmen des Standardersatzbedarfs: Der turnusmäßige Austausch von Endgeräten erfolgt unabhängig über alle Modellinien. Der Tausch erfolgt durch Vor-Ort-Techniker:in.

Anwender:innenanfragen, Störungsmeldung
UHD – User Help Desk
Der Anwender:innen-Support für Arbeitsplatz-Modelllinien ist im ersten Schritt [1. Level Support] unabhängig vom eingesetzten Endgerät bzw. Betriebssystem. Sollte der Erstlösungsversuch nicht zum Ziel führen, übernehmen im Anschluss die zuständigen spezialisierten Supportgruppen [2./3. Level Support] die Bearbeitung.

Fernwartung statt Vor-Ort-Hilfe
Remote-Support
Fernwartung ist der regelhafte Weg der direkten Unterstützung von Anwender:innen durch den Anwender:innen-Support z. B. für allgemeine Fragestellungen oder die Störungsbearbeitung.

Vor-Ort-Techniker
Field Service
Der Einsatz von Techniker:innen vor Ort ist primär für den Aufbau, Tausch und Abbau von Endgeräten bei den Anwender:innen zuständig.

Initiale Einrichtung
Automatische Installation
Hier erfolgt die standardisierte Grundinstallation der Endgeräte. Dies erfolgt vorab zentral vor Auslieferung des Gerätes. Die abschließende Installationen [Updates, Patches und auch Konfigurationsanpassungen] laufen im Anschluss vor Ort bei dem:der Kund:in ohne Interaktion mit Anwender:innen ab. Ein:e Vor-Ort-Techniker:in [Field Service] stellt lediglich beim Aufbau der Geräte sicher, dass eine Erreichbarkeit [Netzwerk] aus der Ferne möglich ist.

Servicekoordination
Die Servicekoordination ist zentrale Ansprechpartner:in zwischen dem:der Kund:in und dem:der IT-Dienstleister:in rund um die Modelllinie. Hier lassen sich Wünsche für die Weiterentwicklung, größere Probleme im Betrieb bei dem:der Kund:in [öffentliche Verwaltung] und die Klärung von Unstimmigkeiten im Tagesgeschäft einsteuern.

4

Technische **Ergebnisse**

Technische **Ergebnisse**

Im Rahmen der von Dataport durchgeführten **Machbarkeitsstudie** im Jahr 2020 zur Einführung einer Linux-Arbeitsplatz-Modelllinie **[vgl. „Ziele und Motivation“]** wurde geprüft, inwieweit ein Verwaltungsarbeitsplatz mit Linux als Betriebssystem realisierbar ist.

Zu diesem Zweck wurde ein strukturierter Anforderungskatalog erstellt und dieser mittels Recherche und technischer Prüfungen abgearbeitet. So konnten die Machbarkeit und die Komplexität jedes Einzelaspekts der Einführung eines Linux-Arbeitsplatzes bewertet werden. Vorlage für die Anforderungen war die Windows-basierte Modelllinie, die um relevante Anforderungen aus den IT-Grundschutz-Bausteinen des Bundesamtes für Sicherheit in der Informationstechnik [BSI] ergänzt wurde.

Überblick **„technische Abschätzung“**

Zusammenfassend wurden im Rahmen der Machbarkeitsstudie 29 technische Arbeitspakete, eingeteilt in die folgenden sechs Kategorien, identifiziert. Die Ergebnisse von drei dieser Arbeitspakete haben informativen Charakter und wurden aus der Gesamtbewertung herausgenommen.

Die betrachteten Kategorien sind:

- **Endgerät, Betriebssystem**
  2 Arbeitspakete
- **Arbeitsplatz: lokale Konfiguration**
  4 Arbeitspakete
- **Arbeitsplatz: Sicherheit**
  5 Arbeitspakete
- **Arbeitsplatz: Anmeldedienste**
  2 Arbeitspakete
- **Zentrale Dienste: Konfiguration, d. h. Systemmanagement**
  6 Arbeitspakete
- **Zentrale Dienste: Kommunikation**
  7 Arbeitspakete

Die im Weiteren betrachteten 26 Arbeitspakete wurden dann bzgl. Aufwand in den Bereichen Integration und Entwicklung bewertet.

Ein besonderes Augenmerk der Analyse war die Fragestellung, inwieweit die aktuelle Infrastruktur der zentralen Dienste im Landesnetz von Schleswig-Holstein angepasst bzw. neu ausgearbeitet werden muss. Zum Zeitpunkt der Analyse wurde von einer Weiternutzung von Teilen der Windows-basierten Server-Backend-Infrastruktur ausgegangen. Daher wurde insbesondere geprüft, wie sich ein Linux-Arbeitsplatz in das bestehende Microsoft-Backend integrieren lässt.

Bereits im Laufe der Analyse zeichnete sich ab, dass bei der Fortschreibung der aktuellen Infrastruktur die Thematik Plattformunabhängigkeit in Bezug auf die Endgeräte und eine betriebssystemübergreifende Client-Kompatibilität eine sehr wichtige Rolle spielen muss.

Zwei Themen konnten als größere Herausforderungen innerhalb der Analyse identifiziert werden:

- **Die Bereitstellung von Fachanwendungen unter Linux** sowie
- **Die Bereitstellung einer Linux-kompatiblen Alternative** zum derzeit genutzten Outlook-Client unter Microsoft Windows

Herausforderung 1: **Fachanwendungen**

Die Bereitstellung von Fachanwendungen unter Linux soll möglichst ohne Medienbruch für die Anwender:innen erfolgen. D.h. auch virtualisierte Anwendungen sollen sich für den:die Anwender:in als in den Desktop eingebettete Anwendungen darstellen. Im Rahmen der Analyse zum Arbeitsplatz wurde deutlich, dass keine vollständige Liste der Fachanwendungen, die in den verschiedenen Landesbehörden genutzt werden, vorliegt. Die Anschaffung von Fachanwendungen unterliegt den jeweiligen Ressorts, nicht dem ZIT Schleswig-Holstein.

EIN GESAMTÜBERBLICK ÜBER ALLE EINGESETZTEN FACHANWENDUNGEN IST VORAUSSETZUNG ZUR ANALYSE DER BEREITSTELLUNGSMÖGLICHKEITEN.

Aktuell wird bei Dataport eine entsprechende Analyse initiiert, um einen möglichst vollständigen Überblick über die Fachanwendungslandschaft der Landesverwaltung Schleswig-Holstein und die einzelnen Softwarearchitekturen zu erhalten.

Herausforderung 2: **Groupware-Applikation à la MS Outlook**

Die zweite Herausforderung ist das Anbieten einer Alternative zum Microsoft-Outlook-Client unter Windows. Ein nicht unwesentlicher Teil des Haupttagesgeschäfts in den jeweiligen Behörden dreht sich um Kommunikation und Koordination. Hierfür hat sich Microsoft Outlook zum Standard entwickelt. Die Bereitstellung eines funktional vergleichbaren Mail- und Groupware-Clients stellt eine der größten Herausforderungen bei einer Umstellung auf einen Linux-Arbeitsplatz dar, insbesondere im Bereich Anwender:innenakzeptanz.

Im Rahmen der Machbarkeitsstudie wurde die Empfehlung ausgesprochen, die Umstellung der E-Mail- und Groupware-Applikation im Rahmen einer Umstellung des E-Mail-Dienstes auf ein Open-Source-Produkt durchzuführen. Problematisch bzgl. der Nutzung von MS Exchange als E-Mail-Dienst in Kombination mit einer Open-Source-E-Mail- und Groupware-Applikation ist das lizenzrechtliche Verbot innerhalb der USA, das von Microsoft patentierte ActiveSync-Protokoll in Open-Source-Anwendungen zu implementieren. Aus diesem Grund gibt es keine Open-Source-E-Mail-/Groupware-Client-Applikation, die man gegen einen MS-Exchange-Dienst verwenden kann.

Problematisch ist diesbzgl. auch, dass für eine Ablösung von MS Outlook nicht nur das Mailprogramm ersetzt, sondern voraussichtlich auch das vollständige Mail- und Kollaborationsbackend MS Exchange durch eine andere Software abgelöst werden muss.

AUSSCHNITTE

Fazits und **Empfehlungen**

Im Folgenden fassen wir die verschiedenen technischen Fazits und Empfehlungen der in 2020 durchgeführten Studie zusammen. Hier ausgelassen werden Themen, auf die in **Kapitel 5 „Themen im Detail“** genauer eingegangen wird.

Verschiedene aktuelle Linux-Distributionen lassen sich auf Notebook-Geräten des Dataport-Gerätewarenkorbs installieren und nutzen. Neu anzubietende Geräte im Dataport-Warenkorb werden zukünftig auf Windows- und Linux-Kompatibilität hin geprüft.

Der Betrieb eines Linux-Geräts in einer Microsoft-Windows-orientierten Infrastruktur ist technisch möglich. Ein Ablösen von Windows-Diensten durch Windows-kompatible Linux-Dienste ist vor allem für den Übergangsmischbetrieb von Windows- und Linux-Clients sinnvoll. Dienste und zentrale Komponenten, die nicht mit Linux kompatibel sind, sollen durch plattformunabhängige Lösungen ersetzt werden. Bei Neuentwicklungen steht die Plattformunabhängigkeit im Fokus.

Die Anwendungen, die den Anwender:innen für das produktive Arbeiten zur Verfügung gestellt werden, werden gängige Softwareprodukte unter Linux sein, die plattformübergreifend verfügbar sind oder die eine hohe Ähnlichkeit bzgl. UI-Design bzw. eine hohe Kompatibilität zu proprietären Produkten aufweisen, z.B.: LibreOffice, Firefox und Chromium. Die Bereitstellung kommerzieller, proprietärer Anwendungen unter Linux in einer Kompatibilitätsschicht [beispielsweise Virtualisierung oder Terminaldienste] wird nur für Fachanwendungen erfolgen.

Die Bereitstellung eines Webbrowsers unter Linux ist unproblematisch. Web-Proxy-Standardeinstellungen sind zentral provisionierbar und erfolgen über das gezielte Platzieren von Konfigurationsdateien. Herausgeber:innen selbstverwalteter CA-Stammzertifikate lassen sich in Chromium und Firefox als vertrauenswürdige Zertifizierungsstellen hinterlegen.

Fortsetzung ▸

Webbrowser sind ein Schlüssel zu betriebssystemunabhängigen Anwendungen. Für die Nutzung weiterer Fachanwendungen ist eine Kompatibilitätsschicht nötig.

Beide Browser lassen sich über Policies systemweit für die Anwender:innen vorkonfigurieren. Einstellungen können auch gezielt für den:die Anwender:in gesperrt werden, sodass immer die systemweite Vorgabe greift.

Bei Weiternutzung von Microsoft Exchange im Backend soll für die erste Version des Linux-Arbeitsplatzes vorerst die Web-Applikation „Outlook on the Web" genutzt werden. Die Anwender:innen erhalten weiterhin alle Funktionen, die sie bereits aus Outlook gewohnt sind und können diese ohne Probleme weiter nutzen. Langfristig soll ein auf Open Source basierender Alternativdienst zu MS Exchange eingesetzt werden, unter Verwendung eines nativen Mail-Clients.

DER EINSATZ VON QUELLOFFENEN DOKUMENTEN-FORMATEN ERLEICHTERT DEN EINSATZ ALTERNATIVER BÜROKOMMUNIKATIONSPRODUKTE UND TRÄGT MASSGEBLICH ZUR DIGITALEN SOUVERÄNITÄT BEI.

Der Funktionsumfang von LibreOffice stellt sich, außer in Details, wie in Microsoft Office dar. Vorhandene Dokumente, die mit Microsoft Office unter Windows im Office-Open-**XML**-Format erstellt wurden, lassen sich auch mit LibreOffice weiterverwenden. Bzgl. der Interoperabilität beim Austausch von Dokumenten zwischen MS Office und LibreOffice besteht eine grundsätzliche Kompatibilität [unter Umständen mit einigen Funktionseinschränkungen bei Verwendung komplexer MS-Office-Funktionen].

eXtensible Markup Language
flexibles, textbasiertes Dateiformat, um komplexe Dokument- und Konfigurationsstrukturen zu implementieren; häufiges Datenaustauschformat u. a. im Web.

Ab Q1/2022 wird bereits vorbereitend eine LibreOffice-Bereitstellung auf der Windows-Modelllinie im Land Schleswig-Holstein erfolgen, wodurch die Office-Produktumstellung [und damit die Übertragung der Dokumentdateien in Open-XML-Formate] bereits unter MS Windows beginnen kann.

Die Fernwartung des Linux-Arbeitsplatzes wird via VNC-Protokoll erfolgen. Eine Enterprise-taugliche Fernwartungsoberfläche für Helpdesk-Mitarbeiter:innen fehlt aktuell noch. Hier ist Entwicklungsarbeit nötig, ggf. in Zusammenarbeit mit bestehenden Open-Source-Projekten. Fernzugriff via SSH auf den Linux-Arbeitsplatz wird innerhalb des jeweiligen Behördennetzes und für den IT-Support möglich sein.

Für das mobile Arbeiten müssen Anwender:innen sich via VPN mit dem Landesnetz verbinden. Die Automatisierung der Zertifikatsbereitstellung [rechnerspezifische SSL-Zertifikate zur kryptografischen Absicherung des VPN-Tunnels] während der vollautomatischen Systeminstallation wird als machbar, aber ggf. zeitaufwendig eingeschätzt.

Im Bereich Systemhärtung wurden bei Dataport intern unterschiedlichste Ansätze zur Härtung des Betriebssystems diskutiert und verschiedene Angriffsszenarien betrachtet. Grundsätzlich wurde unterschieden zwischen Offline- und Online-Bedrohungen. Bzgl. der Offline-Bedrohungen wurden sowohl Angriffsszenarien vor dem Systemstart als auch diverse Angriffsszenarien [Online-Bedrohungen] nach dem Systemstart betrachtet.

Eines der im Detail geprüften Verfahren war die während einer automatisierten Bereitstellung konfigurierte Festplattenverschlüsselung. Die Komplettverschlüsselung von lokalen Datenträgern schützt vor Offline-Bedrohungen und ist ein Muss der Systemhärtung von mobilen Arbeitsplätzen. Die Möglichkeit einer automatischen Systemeinrichtung mit Ablage/Bezug von Verschlüsselungs-Passphrases in/aus Active Directory in Kombination mit TPM-Schutz wurde erfolgreich in einem Testprojekt geprüft und bestätigt.

Zum Schutz vor Online-Bedrohungen wird der Linux-Arbeitsplatz in jedem Fall über eine zentral konfigurierbare, lokale Firewall verfügen. Hierfür wird voraussichtlich die Standard-Firewall der verwendeten Linux-Distribution zum Einsatz kommen.


© pexels.com / Yan Krukov


© Unsplash.com / Priscilla Du Preez

Themen im Detail

5

Themen im **Detail**

THEMA 1

Bereitstellung nativer **Windows-[Fach-] Anwendungen**

Auf den Arbeitsplätzen der öffentlichen Verwaltung in Schleswig-Holstein ist das Betriebssystem Microsoft Windows seit Jahrzehnten als Standard in Form einer eigenen Arbeitsplatz-Modelllinie etabliert. Im Gegensatz zu dieser homogenen Betriebssystemumgebung stellt sich die Anwendungslandschaft in Bezug auf die Vielfalt von Softwarearchitekturen der genutzten Fachverfahren sehr heterogen dar.

Die Anwendungslandschaft, die sich bisher am De-facto-Standard „Windows-Betriebssystem" orientiert hat, besteht zu einem hohen Anteil aus nativen Windows-[Fach-]Anwendungen. Diese lassen sich aktuell nicht ohne Alternativen in der Bereitstellung auf einem Linux-Betriebssystem nutzen.

Generell haben sich Softwarearchitekturen in den letzten Jahren in Bezug auf die Plattformunabhängigkeit zur Betriebsumgebung [Betriebssystem und Endgerätetyp] stark weiterentwickelt. Durchgesetzt haben sich plattformunabhängige Softwarearchitekturen, die web-basiert gleichermaßen auf Tablets, Handys und Computern bedient werden können. Bzgl. der Plattformunabhängigkeit in der Fachverfahrenslandschaft zeichnet sich heute ein weitaus besseres Bild ab als noch vor wenigen Jahren. Dennoch wird die Integration von Fachverfahren in den Linux-Arbeitsplatz als eines der arbeitsintensivsten Teilprojekte bewertet.

FACHANWENDUNGEN SIND EIN ENTSCHEIDENDER ASPEKT BEI DER EINFÜHRUNG EINES LINUX-BASIERTEN VERWALTUNGS-ARBEITSPLATZES. DIE INTEGRATION NATIVER WINDOWS-FACHANWENDUNGEN IST EINE KOMPLEXE HERAUSFORDERUNG.

Weitverbreitete Fachanwendungen, die aktuell nur nativ unter dem Windows-Betriebssystem lauffähig sind, müssen langfristig auf neue, plattformunabhängige Architekturen mit moderner Bedienoberfläche umgestellt werden. Dies erfordert ein grundlegendes Neudesign und einen hohen Entwicklungs- und Kostenaufwand aufseiten der Softwareanbieter:innen.

Bisherige Monolith-Softwarekonzepte in der IT-Landschaft von Verwaltungseinrichtungen weisen häufig eine starke Abhängigkeit von der Betriebsumgebung [Windows Betriebssystem, PC-ähnliches Endgerät] auf. Es ist zu erwarten, dass solche klassischen Softwaredesigns langfristig durch neue Softwarearchitekturen [z. B. Web-Services, Entwicklung auf Basis plattformübergreifender Toolkits wie z. B. **Qt**, UI-Konzepte für touchbasierte Endgeräte etc.] flächendeckend in der Verwaltungslandschaft abgelöst werden.

Für den Übergangszeitraum bedarf es für weitverbreitete Fachanwendungen einer Zwischenlösung, um von den vorhandenen, meist nativen Windows-Anwendungen hin zu den o. g. neuen Softwarearchitekturen überzuleiten. Eine nicht lokale Bereitstellung solcher Windows-basierten Fachverfahrensanwendungen [im Weiteren als „alternative Bereitstellung" bezeichnet] wird als eine mögliche Zwischenlösung gesehen und kann als Brücke für genau diesen Wandel der Betriebsumgebungen und auch der Softwarearchitekturen dienen.

Fachanwendungen, die hingegen sehr spezifisch sind, müssen wahrscheinlich langfristig auf einer Windows-[ähnlichen] Plattform weiterbetrieben werden. Eine alternative Bereitstellung wird hier keine Zwischenlösung sein, sondern die Standardvorgehensweise. Grundsätzlich wird zu diskutieren sein, ob die Methoden der alternativen Bereitstellung nicht auch gleich dafür genutzt werden sollten, die IT-Verfahrenslandschaft in Schleswig-Holstein flächig stark zu vereinheitlichen und zu standardisieren. Nicht jede Anwendung ist dafür geeignet, als Web-Service portiert und bereitgestellt zu werden. Die Bereitstellung einer solchen Desktop-Anwendung [egal ob auf Windows oder Linux lauffähig] muss ggf. langfristig möglich bleiben. Die hier diskutierten Methoden der alternativen Bereitstellung könnten langfristig neben Fachverfahren im Web als neues Architekturkonzept für Fachanwendungen aufgefasst werden.

Im folgenden Abschnitt werden verschiedene technische Methoden der alternativen Bereitstellung erläutert und deren Einsatzmöglichkeiten aufgezeigt.

Derzeit sind nur wenige **Fachanwendungen** nativ auf einen betriebssystem-unabhängigen Betrieb ausgelegt.

Qt

Bibliothek zur Entwicklung grafischer, plattformübergreifender Anwendungen **qt.io**

Technologien für eine alternative Bereitstellung

Für den Betrieb von Fachanwendungen, die nicht nativ unter einem Linux-Betriebssystem lauffähig sind, gibt es verschiedene technische Möglichkeiten. Alle haben gemein, dass sie der nativen Windows-Fachanwendung eine passende Betriebsumgebung zur Verfügung stellen. Dies hat den Vorteil, dass keine Anpassungen an der Fachanwendung notwendig sind. Diese Umgebung wird dann über den Arbeitsplatz genutzt. Generell bringen diese Alternativen eine unterschiedliche Ressourcennutzung und Änderungen an den Lizenzkosten mit sich. Je nach Bereitstellungstyp kommen aber neben Einschränkungen auch neue Möglichkeiten hinzu, z.B. eine bessere Verwaltung von Fachanwendungen oder eine effektivere Ressourcennutzung.

Die folgenden vier Bereitstellungsmöglichkeiten lassen sich unterscheiden:

Desktop-Virtualisierung
Virtual-Desktop-Infrastruktur, Terminalservices

Grundsätzlich unterscheidet man bei der Desktop-Virtualisierung die Begrifflichkeiten Virtual-Desktop-Infrastruktur [VDI] und Terminalservices. Technisch sind hier Mischformen möglich. Daher soll wie folgt unterschieden werden: Bei VDI wird den Anwender:innen eine eigene virtuelle Desktop-Betriebssysteminstanz zur Verfügung gestellt z.B. Windows 10. Bei Terminalservices erhalten Anwender:innen einen Desktop von einem Mehrbenutzer-Server-Betriebssystem z.B. Windows Server 2016.

Bei beiden Technologien wird ein komplettes Windows-Betriebssystem als Betriebsumgebung bereitgestellt. Mit dieser ist es möglich, eine Fachanwendung ohne Einschränkungen [virtuell] auszuführen. Beim Einsatz von Fachanwendungen auf Terminalservern ist auf die Kompatibilität der Software in einer solchen Umgebung zu achten.

Bei VDI wird die Windows-Umgebung in Form einer virtuellen Maschine [VM] auf einem Serversystem, dem sogenannten Hypervisor, bereitgestellt. Auf dem Arbeitsplatz wird mithilfe einer Software eine Vermittlungsinstanz hergestellt, die mit dem entfernten virtuellen Arbeitsplatz kommuniziert und die Bildschirmdarstellung übernimmt. Die Anwender:innen arbeiten somit direkt auf dem virtuellen System.

Lokale Desktop-Virtualisierung
Hypervisor auf dem Arbeitsplatz

Bei der lokalen Desktop-Virtualisierung ist der Hypervisor direkt auf dem Arbeitsplatz installiert [z.B. VMware Workstation]. Den Anwender:innen wird ein komplettes Betriebssystem innerhalb des Arbeitsplatzes bereitgestellt. Der größte Unterschied liegt hier in der Verwaltung der virtuellen Maschine [VM] und dem Ressourcenverbrauch. Für den:die Anwender:in ist der Unterschied zwischen der entfernten und lokalen Desktop-Virtualisierung nicht unbedingt ersichtlich.

Publizierte Anwendung

Die Technologie für publizierte Anwendungen setzt auf der Desktop-Virtualisierung auf. Bei dieser Bereitstellungsmethode wird dem:der Anwender:in kein ganzes Betriebssystem zur Verfügung gestellt, sondern nur die eigentliche Fachanwendung. Technisch funktioniert dies identisch zur Desktop-Virtualisierung mit einer Vermittlungsinstanz, die die Kommunikation und Darstellung der Fachanwendung übernimmt. Für die Anwender:innen entsteht kein sichtbarer Unterschied zu einer lokal installierten Fachanwendung. Auch Verknüpfungen zwischen Fachverfahren lassen sich mit dieser Bereitstellungsmethode abbilden.

Kompatibilitätsschicht für Windows-Anwendungen
Lokale Anwendung

Der letzte Bereitstellungstyp ist eine Einzellösung für Unix-Betriebssysteme, um Windows-Anwendungen auf diesen Plattformen zu betreiben. Konkret wird hier das Open-Source-Produkt „Wine“ erläutert, um einen vollständigen Blick auf alternative Bereitstellungsmöglichkeiten abzubilden. Der Produktname Wine setzt sich wie folgt zusammen: Wine Is Not an Emulator. Damit ist gemeint, dass Wine keine Emulation sein möchte, sondern sich als Laufzeitumgebung für Windows-Betriebssysteme versteht. Die Aufrufe der Laufzeitumgebung werden nicht durch eigene Programmierungen nachgebildet, sondern direkt an die jeweilige Systemkomponente weitergereicht.

Allerdings basiert diese Bereitstellungsmethode nicht auf einem nativen Windows-Betriebssystem. Ob und welche Auswirkungen dies auf die verschiedenen Fachanwendungen hat, lässt sich nur im Einzelfall überprüfen.

Vier Schritte zu plattformunabhängigen Anwendungen

1 Inventur der **Anwendungslandschaft**

Als ersten Schritt noch vor der Analyse zur Plattformunabhängigkeit einzelner [Fach-]Anwendungen ist es notwendig, die gesamte Anwendungslandschaft der jeweiligen Verwaltung zu analysieren. Daraus ergibt sich ein Gesamtbild über die Komplexität, dessen Ergebnis starken Einfluss auf die passende Auswahl der alternativen Bereitstellungsarten hat.

Eine Bewertung, ob eine Fachanwendung weitere Betriebsplattformen neben Microsoft Windows als Betriebssystem unterstützt, muss in einer Einzelbetrachtung erfolgen. Diese Einzelbetrachtung kann sich je nach Fachanwendung, Anbieter:in und Informationslage sehr zeitintensiv gestalten.

2 Auswahl der optimalen **technischen Bereitstellung**

Auf Grundlage der Analyse der Anwendungslandschaft kann im nächsten Schritt eine spezifische Prüfung bzgl. einer Zuordnung zu Lösungsalternativen in der Bereitstellung erfolgen. Im Idealfall ist durch die vorherige Analyse schon vertieftes Wissen zu der Funktionsweise der Fachanwendung bekannt. Andernfalls muss an dieser Stelle eine vertiefte, technische Betrachtung durchgeführt werden, um die sinnvollste Betriebsart für den jeweiligen Anwendungstyp auszuwählen.

Mit diesem Vorgehen können die Einzelbetrachtungen im Anschluss nach Priorität, Roadmap oder Bedeutung für die jeweilige Verwaltung gezielt angegangen werden, um die Fachanwendungen geordnet und planbar auf einer Linux-Arbeitsplatz Modellinie zu überführen.

3 Bereitstellung der **Windows-Anwendungen**

Dataport bietet seinen Kund:innen zentrale Infrastrukturdienste an, um Fachanwendungen über „Desktop-Virtualisierung" oder „Anwendungs-Virtualisierung" bereitzustellen. Mit diesen Diensten ist es möglich, native Windows-Anwendungen auf einem Linux-Desktop bereitzustellen.

4 Fortschreibung der **Anwendungslandschaft**

Durch die Analyse in den Schritten 1 und 2 liegen nun wertvolle Informationen für eine zielgerichtete IT-Strategie bezogen auf den Anwendungsbetrieb [z.B. Einschränkungen, plattformübergreifende Ansätze, konkrete Roadmaps von Produkten] vor. Auf Grundlage des Istzustands lassen sich nun strategische Entscheidungen für die gezielte Fortentwicklung der Anwendungslandschaft und den Anwendungsbetrieb ableiten.

FACHANWENDUNGSBEISPIEL 1

Die **elektronische Akte**

Für die elektronische Aktenhaltung und die digitale Abbildung der Umlaufmappe wird auf beinahe allen Verwaltungsarbeitsplätzen in Schleswig-Holstein eine einheitliche Software eingesetzt. Diese ist als das Fachverfahren mit der meisten Verbreitung in der IT-Landschaft der Landesverwaltung anzusehen. Für die Nutzung wird auf zwei Client-Varianten gesetzt: eine nativ auf dem Endgerät installierte Anwendung und eine Web-Applikation [Zugriff über den Webbrowser].

Die installierte Client-Anwendung setzt dabei auf das .NET-Framework als Laufzeitumgebung. Das ActiveX-Objekt des zugehörigen Web-Clients wird für die Nutzung der nativen Client-Anwendung benötigt. Eine Lauffähigkeit mit der quelloffenen .NET-Implementierung Mono sollte getestet werden. Vom Hersteller wird aktuell nur der Betrieb auf Windows-basierten Endgeräten unterstützt.

Die über den Webbrowser erreichbare Client-Anwendung wird zu 75 % über Webtechnologien realisiert. Für die Nutzung wird zwingend ein ActiveX-Objekt benötigt, welches die restlichen 25 % zur Verfügung stellt. Der einzige, vom Hersteller unterstützte Webbrowser ist derzeit der Internet Explorer unter Windows.

Der Fachverfahrenshersteller hat bereits in Aussicht gestellt, dass zukünftige Versionen der Anwendung in HTML5 veröffentlicht werden und auf Chromium-basierten Browsern offizielle Unterstützung bekommen werden. Zu einer Lauffähigkeit auf weiteren Browsern mit alternativer Engine gibt es bisher keine offizielle Herstelleraussage.

THEMA 2

Offline-Fähigkeit des Endgeräts

[6] **Office**
Öffnen, Bearbeiten und Speichern von Dokumenten

[7] **E-Mails**
Erstellung neuer Nachrichten, Einsichtnahme in bereits erhaltene Nachrichten

[8] **Groupware**
Einsichtnahme Kalender, Kontakte, Aufgaben sowie Anlegen neuer Einträge

[9] **Corporate-Netzwerk**
Allgemein ein Unternehmensnetzwerk [bzw. Behördennetzwerk], in dem eine Dienstinfrastruktur für Endgeräte bereitgestellt ist. Meist gelten in solchen Netzwerkumgebungen strengere Richtlinien, als sie aus dem Privatbereich bekannt sind. Arbeitsplätze im Corporate-Netzwerk sind stark auf die Dienstinfrastruktur abgestimmt und können je nach IT-Richtlinien im Unternehmen ggf. gar nicht außerhalb der Unternehmensstruktur produktiv genutzt werden.

Für die zu konzipierende Linux-Arbeitsplatz Modellinie der Landesverwaltung Schleswig-Holstein besteht die Anforderung, bzgl. der Arbeitsmethoden **Office**[6], **E-Mails**[7] und **Groupware**[8] weitestgehend produktiv arbeitsfähig zu bleiben, auch wenn vorübergehend keine Verbindung zum **Corporate-Netzwerk**[9] [Intranet oder VPN] der jeweiligen Behörde besteht bzw. auch wenn mit dem Endgerät das Corporate-Netzwerk verlassen wird und z. B. in ein anderes WLAN gewechselt wird.

Zielvorgabe dieser sogenannten Anforderung „Offline-Fähigkeit des Endgeräts" ist es, Anwender:innen, auch bei „Netzwerkschwankungen" stets maximal arbeitsfähig zu halten. Was genau verbirgt sich dahinter?

Offline-Fähigkeit im privaten Umfeld

Privatanwender:innen nutzen mit ihren mobilen Endgeräten häufig unterschiedliche Netzwerke und kennen auch Phasen ohne Internetverbindung. Auf privaten Endgeräten ist vorübergehende Offline-Fähigkeit quasi Normalität. Das Endgerät an sich speichert alle Daten primär lokal und damit sind alle Anwendungen, die nicht von verfügbarem Internet abhängen, offline benutzbar. Die Kombination von Anwendungen und der jeweiligen persönlichen Nutzungsweise des Endgeräts entscheidet darüber, in welchem Ausmaß Anwender:innen mit privaten Endgeräten auch ohne Internetzugriff produktiv agieren können. Erfahrene Anwender:innen können sich ergänzend mit Daten und Informationen ausstatten, um längere Offline-Phasen geplant zu überbrücken. Die persönliche Strategie für das Überbrücken von Offline-Phasen wird sehr individuell gestaltet.

Offline-Fähigkeit im Enterprise-Umfeld

Die Implementierung einer Offline-Fähigkeit von Endgeräten im Enterprise-Umfeld [Unternehmens-IT, IT der öffentlichen Verwaltung etc.] hingegen ist eine vielschichtige Thematik und unter GNU/Linux für den Enterprise-Kontext noch nicht weit erprobt. Anders als im privaten Bereich kann von Anwender:innen im Unternehmen [bzw. in der öffentlichen Verwaltung] nicht erwartet werden, die genaue Funktionsweise des Endgeräts und der nachgeschalteten Infrastruktur zu durchdringen, um sich dann selbst Strategien für Offline-Phasen am Endgerät „auszudenken". Im Enterprise-Umfeld muss den Anwender:innen ein Endgerät bereitgestellt werden, welches bzgl. der verfügbaren Netzwerkkonnektivität eine transparente Arbeitsweise erlaubt. Gleichzeitig wird es nötig sein, Anwender:innen für das Arbeiten im Offline-Betrieb am Linux-Endgerät zu schulen. Die Anforderung „Offline-Fähigkeit des Endgeräts" muss somit mit einer Kombination aus technischen und organisatorischen Maßnahmen beantwortet werden.

Der technische Aspekt einer „Offline-Fähigkeit des Endgeräts" ist unter Linux voraussichtlich über das Zusammenspiel verschiedener Tools und Dienste, die das Endgerät in einzelnen Bereichen „offline-fähig" machen, zu realisieren [Baukastenprinzip]. Es gibt für diese Anforderung unter Linux keine Komplettlösung. Die Offline-Fähigkeit der Linux-Arbeitsplatz-Modelllinie wird aus der Summe verschiedener Teilprojekte resultieren. Die Anforderung des Gesamtbilds „Offline-Fähigkeit des Endgeräts" an den neu zu konzipierenden Linux-Arbeitsplatz orientiert sich dabei an den verschiedenen, verfügbaren Offline-Funktionalitäten der aktuell betriebenen Modelllinie [basierend auf Microsoft Windows 10]. Für die Linux-Arbeitsplatz-Modelllinie soll [auch aus Sicht der Anwender:innen] eine gleichwertige Enterprise-Offline-Fähigkeit erarbeitet werden. **Diese Aufgabenstellung wird als sehr umfangreich eingestuft.**[10]

Online vs. Offline

Um Lösungsansätze für „Offline-Fähigkeit des Endgeräts" im Detail formulieren zu können, gilt es zunächst, herauszuarbeiten, was mit „online" und „offline" eigentlich gemeint ist, welche Abstufungen dazwischen unterschieden werden müssen und welche genauen Funktionen während der unterschiedenen [Semi-]Offline-Phasen noch verfügbar sein sollen.

A. Das Endgerät ist „online" und eingebucht im eigenen Corporate-Netzwerk. Alle für das Endgerät vorgesehenen Infrastrukturdienste [Dateiablage, Internet-Gateway, Konfigurationsmanagement etc.] der Enterprise-IT-Umgebung sind für das Endgerät verfügbar, Anwender:innen können den vollständigen Funktionsumfang des Endgeräts nutzen und sind bestmöglich durch die Sicherheitsmechanismen der Corporate-IT-Umgebung geschützt [Firewall, Web-Proxy mit Virenschutz, Bereitstellung von Sicherheitsupdates etc.].

B. Das Endgerät ist „online" und eingebucht in einem fremden Netzwerk mit vollständigem Zugriff aufs Internet [z. B. privates Netzwerk der Mitarbeiter:innen]. Die Dienste der Enterprise-IT-Umgebung sind nicht verfügbar, können aber über VPN erreichbar gemacht werden. Nach Aufbau des VPN-Zugangs zum Corporate-Netzwerk ist das Endgerät in vollständigem Funktionsumfang nutzbar und geschützt.

C. Das Endgerät ist „online", aber eingebucht in einem fremden Netzwerk mit limitiertem Internetzugriff [z. B. Gast-WLAN eines anderen Unternehmens oder einer anderen Behörde]. Die Infrastrukturdienste des Corporate-Netzwerks sind nicht verfügbar und können auch über VPN nicht erreichbar gemacht werden. Das Endgerät ist ggf. nicht vollständig nutzbar.

D. Das Endgerät ist vollständig „offline", d. h., es besteht keinerlei Verbindung zum Internet. Das Endgerät ist für einige Arbeitsaufgaben ggf. nicht nutzbar.

Die Betriebsmodi **A** und **B** sind für die Betrachtung einer Offline-Fähigkeit von Endgeräten nicht relevant. Die Geräte werden in diesen Betriebsmodi in vollem Funktionsumfang nutzbar sein.

Im Folgenden soll der Fokus der Betrachtung auf die Betriebsmodi **C** und **D** begrenzt werden:

- **„Offline-Fähigkeit"** bei teilweise verfügbarer Internetverbindung [vgl. Betriebsmodus C], im weiteren Text durch „eingeschränkte Internetkonnektivität" referenziert]
- **„Offline-Fähigkeit"** bei Fehlen jeglicher Internetkonnektivität [vgl. Betriebsmodus D], im weiteren Text durch „vollständig offline" referenziert]

Bausteine für die Bereitstellung von Offline-Fähigkeit

Im Folgenden soll nun bzgl. der Anforderung „Offline-Fähigkeit des Endgeräts" [vgl. S. 22] insbesondere auf die systemnahen Funktionen des Linux-Arbeitsplatzes und dessen Interaktionen

Fortsetzung ▸

[10] **Offline-Verfügbarkeit**
Nur wenige recherchierte Betriebsmodelle von Linux-Arbeitsplätzen im Unternehmen sehen das Feature „Offline-Fähigkeit des Endgeräts" überhaupt vor. In Corporate-IT-Umgebungen [z. B. Universitäten, Forschungseinrichtungen etc.] ist der Betrieb von Linux-Arbeitsplätzen meist auf eine 100 %ige Verfügbarkeit einer internen Netzwerk-Infrastruktur ausgelegt. Oder es werden den Mitarbeiter:innen Arbeitsplatzgeräte bereitgestellt, die dann durch die Mitarbeiter:innen selbst zu administrieren sind.

mit den zugehörigen Infrastrukturdiensten des Corporate-Netzwerks eingegangen werden:

- **Anmeldeverfahren**
- **Synchronisation von Speicherorten**
- **Benutzer:innenprofile [insbesondere Profil-Roaming]**
- **Konfigurationsmanagement und Softwareaktualisierungen**

Abschließend wird auch noch die nicht systemnahe

- **Offline-Bereitstellung einzelner Fachverfahren**

betrachtet werden.

Anmeldeverfahren

Wichtig für einen mobilen Arbeitsplatz ist die Offline-Fähigkeit gegenüber dem in der Infrastruktur bereitgestellten Anmeldedienst. Anwender:innen auf Endgeräten im Corporate-Netzwerk müssen sich gegen ein Identity-und-Access-Management[IAM]-System authentifizieren und autorisieren. Die zugehörigen Informationen von Benutzer:innen wie auch die Zugangsdaten der Anwender:innen müssen offline auf dem Endgerät vorgehalten werden können. Auch bei fehlender Verbindung zum Corporate-Netzwerk muss eine Anmeldung am Arbeitsplatzsystem bzw. das Entsperren der Arbeitsoberfläche möglich sein.

In der Machbarkeitsstudie aus dem Jahr 2020 [vgl. S. 7] wurden detaillierte Vorschläge zur Implementierung von Offline-Fähigkeit des Linux-Endgeräts gegenüber dem aktuell genutzten Anmeldeverfahren [MS Active Directory] ausgearbeitet. Empfohlene Open-Source-Softwarekomponenten für die Umsetzung sind der „System Security Service Daemon" [SSSD] und das PAM-Modul „libpam-mklocaluser". Der SSSD läuft lokal auf dem Endgerät, stellt die Brücke zwischen IAM-System [ActiveDirectory oder LDAP-Dienst bzw. Kerberos] und dem Linux-Arbeitsplatzsystem dar und ist in der Lage, Anmeldedaten [Name und Kennwort der Benutzer:innen] für einen temporären Zeitraum zwischenzuspeichern [sogenanntes Caching]. Ebenfalls macht der SSSD die Gruppenzugehörigkeiten von Benutzer:innen des IAM-Systems auf dem Endgerät [offline] verfügbar. Die Erstanmeldung eine:r Anwender:in am Endgerät muss im Corporate-Netzwerk erfolgen, danach kann sich dieselbe Person auch **vollständig offline oder bei eingeschränkter Internetkonnektivität** am Gerät anmelden. Die Ergänzung des SSSD durch libpam-mklocaluser sorgt dafür, dass Corporate-Benutzer:innenkonten auf dem Endgerät vollständig persistent angelegt werden.

Synchronisation
von Speicherorten

Arbeitsdaten [Dokumente, Bilder etc.] sind zu unterscheiden von Daten des Benutzer:innenprofils [d.h. Dateien und Ordner, in denen Anwendungen ihre Einstellungen speichern]. Beide Datentypen werden auf Linux-Systemen im sogenannten HOME-Verzeichnis [das persönliche Verzeichnis eine:r Anwender:in] abgelegt.

Es wird im Folgenden zunächst der Fokus auf die Arbeitsdaten gelegt, im nächsten Abschnitt [vgl. S. 47] wird anschließend die Thematik der Synchronisation von Benutzer:innenprofilen vertieft. Eine wichtige Anforderung im Corporate-Netzwerk ist, dass Arbeitsdaten möglichst in Echtzeit serverseitig zentral gespeichert werden [Schutz vor Datenverlust auf dem Endgerät, sofortige Bereitstellung der Arbeitsdaten für Kolleg:innen]. Arbeitsdaten können persönliche Dateien von Anwender:innen sein, aber auch Dateien, die in Gruppenordnern abgelegt werden und von mehreren Anwender:innen aufgerufen und bearbeitet werden können. Was ist hier bzgl. Offline-Fähigkeit zu bedenken?

Grundsätzlich wird empfohlen, insbesondere aus Gründen der Performanz, das Endgerät als primären Speicherort für persönliche Arbeitsdaten [eigene Dokumente, Bilder etc.] zu nutzen.[11] Bei bestehender Internetkonnektivität [direkt im Corporate-Netzwerk bzw. per VPN-Verbindung zum Corporate-Netzwerk] werden die Arbeitsdaten dann im Hintergrund quasi in Echtzeit mit einem Speicherort auf einem zentralen Server abgeglichen. Synchronisationskonflikte sind beim fortwährenden Arbeiten mit demselben Endgerät für persönliche Dateien und Ordner unwahrscheinlich.

[11] **Arbeitsdaten-speicherung**
Die andere Möglichkeit wäre, Arbeitsdaten primär serverseitig zu speichern und dann ggf. in Offline-Kopie auf dem Endgerät bereitzuhalten. Je nach Bandbreite und Latenz der Netzwerkverbindung kann es hier zu Einschränkungen beim Arbeiten kommen.

Die Funktionalität „Synchronisation von Arbeitsdaten" hat auf der aktuell eingesetzten Windows-Modelllinie in Schleswig-Holstein bereits mehrere Iterationen von verschiedenen Lösungsansätzen durchlaufen. Die für die Linux-Arbeitsplatzmodelllinie aktuell favorisierte Lösung wurde in Anlehnung an die aktuelle Vorgehensweise bei der Windows-Modelllinie [Https-Synchronisation in Microsoft Windows Workfolders] erarbeitet. Die Linux-Arbeitsplatz-Modelllinie wird serverseitig einen eigenen Dienst hierfür benötigen, da MS Windows Workfolders keine Linux-Clients unterstützt. Mögliche OSS-Produkte für einen solchen Dienst [sogenannte On-Premise-Cloud-Speicher] sind Produkte wie Nextcloud, ownCloud, Seafile oder SyncThing. Aber auch eine eigene Low-Level-Implementierung auf Basis der Tools „rsync" oder „unison" ist denkbar. Ein Umstieg auf einen solchen Synchronisationsmechanismus ist bereits vor der Arbeitsplatzumstellung auf Linux möglich, da die genannten Produkte sowohl Linux- als auch Windows-Clients unterstützen.

Der Zugriff auf die persönlichen Arbeitsdaten [lesend und schreibend] ist mit einem solchen Ansatz stets möglich, auch wenn das Gerät **vollständig offline** ist oder mit **eingeschränkter Internetkonnektivität** gearbeitet werden muss. Bei länger andauerndem Offline-Betrieb zeichnet sich ein steigendes Risiko von Datenverlust ab [z.B. bei Defekt des Endgeräts sowie Verlust oder Diebstahl].

Für die bisherige Modelllinie ist eine Offline-Nutzung von Gruppenlaufwerken in der Regel nicht vorgesehen, da sich die Gefahr von Konflikten bei gemeinsamer Bearbeitung von Dateien für den Offline-Fall nicht beherrschen lässt. Ähnliches wird auch für die Linux-Arbeitsplatz-Modelllinie gelten. D.h., für die Offline-Nutzung und -Bearbeitung von Gruppendaten müssen organisatorische Strategien erarbeitet und in Form von Schulungen den Anwender:innen vermittelt werden.

Profile der Benutzer:innen
insbesondere Profilroaming der Benutzer:innen

Der Begriff „Benutzer:innenprofil" ist eigentlich ein Terminus aus der Microsoft-Windows-Welt. Eine Übertragung des Begriffs in die Linux-Welt ist möglich: Als Benutzer:innenprofil soll in dieser Betrachtung die Gesamtheit aller für die Benutzer:innen spezifischen Programmeinstellungen verstanden werden. Diese werden standardmäßig unter Linux neben den Arbeitsdaten im HOME-Verzeichnis der Benutzer:innen in versteckten Ordnern und Dateien gespeichert.

Anforderung an eine Enterprise-Arbeitsplatz-Modelllinie für die Landesverwaltung Schleswig-Holstein ist ein infrastrukturweites Benutzer:innen-Profilmanagement. Hierzu gehört insbesondere eine Profilsynchronisation auf zentrale Speicherorte in möglichst regelmäßigen Intervallen. Dies dient einerseits der Datensicherung, andererseits ist dies wichtig für die Beibehaltung des Benutzer:innenprofils bei Wechsel des Arbeitsplatzgeräts [sogenanntes Profil-Roaming]. Für die Linux-Arbeitsplatz-Modelllinie gilt es, für möglichst viele der benutzer:innenspezifischen Programmeinstellungen eine Synchronisationsmethode zu entwickeln und diese in das infrastrukturelle Benutzer:innen-Profilmanagement zu integrieren. Ein Nebeneffekt des Profilmanagements für Benutzer:innen wird die „Offline-Fähigkeit des Endgeräts" bzgl. individueller Einstellungen der Benutzer:innen sein.

Für Linux-Benutzer:innenprofile [ähnlich wie für die Arbeitsdaten, vgl. S.46] soll das Endgerät als primärer Speicherort verwendet werden. Anders als bei den Arbeitsdaten hat der Abgleich von Profildateien nicht permanent, sondern nur bei An- und Abmeldung zu erfolgen.

Das Arbeiten mit Anwendungen und das Ablegen von Anwendungseinstellungen ist grundsätzlich immer möglich, wenn die Profildaten primär lokal gespeichert werden, d.h. insbesondere auch, wenn das Endgerät **vollständig offline** ist oder mit **eingeschränkter Internetkonnektivität** betrieben wird. Die Komplexität liegt in der fehlerfreien Synchronisation dieser Einstellungsinformationen zu einem zentralen Speicherort, ohne dass Anwender:innen davon bei ihrer Arbeit beeinträchtigt werden oder in den Vorgang eingreifen müssen.

Kritische **Betrachtung**

Die Thematik der Benutzer:innenprofilsynchronisation wirft auch Fragen auf: Braucht es Profilsynchronisation auf einem Linux-basierten Arbeitsplatz wirklich? Und wenn ja, warum genau? Lassen sich die hinter Benutzer:innenprofilsynchronisation versteckten eigentlichen Anforderungen nicht technisch auch ganz anders realisieren?

SMB
Das Server Message Block Protokoll dient als Client-/Server-Protokoll für die Freigabe von Dateien über das Netzwerk.

[Technische] Gründe für Benutzer:innenprofilsynchronisation:

- **Datensicherung von Einstellungen der Benutzer:innen** eines individuellen Endgeräts
- **Roaming der Benutzer:innen** [ein:e Anwender:in wechselt regelmäßig seine:ihre offlinefähige Arbeitsstation, d.h., wechselt zwischen verschiedenen Notebooks]; wie wahrscheinlich ist dieses Nutzungsszenario?
- **Administrator:innen melden sich häufig an verschiedenen Endgeräten im Corporate-Netzwerk** mit ihren persönlichen Benutzer:innenkonten [oder auch mit Testkonten] an; wie wichtig sind hier Roaming-Profile?

Die Implementierung eines reibungsfrei funktionierenden Profil-Roamings ist aufgrund der zu erwartenden hohen Entwicklungs- und Integrationskosten genau zu betrachten.
Folgende alternative Strategien sind denkbar:

- **Profil-Roaming:** Echtes Benutzer:innenprofil-Roaming wird meist nur auf stationären Geräten benötigt. [Mitarbeiter:innen tauschen selten ihre Notebooks hin und her]. Diese stationären Geräte sind in der Regel über LAN mit dem Netzwerk verbunden und somit permanent online. Hier wären ggf. vollwertige Netzwerk-Home-Verzeichnisse [z.B. auf NFS- oder **SMB**-Servern] der sinnvollere Lösungsansatz. D.h., es müsste innerhalb der Linux-Arbeitsplatz-Modelllinie unterschieden werden zwischen mobilen und nicht mobilen Endgeräten
- **Datensicherung:** Im Corporate-Netzwerk könnte es einen Dienst für Client-Datensicherung geben, der mehrmals täglich versuchen würde, alle Endgeräte im Netz zu erreichen. Dieser Dienst würde die Arbeitsdaten und die Profildaten sichern. Profildaten können nicht im laufenden Betrieb gesichert werden, sondern nur, wenn der:die Benutzer:in nicht am Gerät angemeldet ist. Als Gegenmaßnahme würde vor bzw. während der Anmeldung am Endgerät eine Staging-Kopie des Benutzer:innenprofils angelegt werden. **Diese würde dann später vom Datensicherungsdienst gesichert werden.**[12]
- **Profile von Administrator:innen:** Die Profile von Administratoren:innen sollten nur temporär auf Endgeräten von Mitarbeiter:innen „auftauchen" und nach Abmeldung zeitnah wieder entfernt werden. Administrator:innen brauchen keine persistenten Profildaten und kommen mit einem zum Zeitpunkt der Anmeldung frisch erstellten Benutzer:innenprofils zurecht.

[12] Selbstbestimmte Datensicherung
Man könnte den Anwender:innen zusätzlich eine grafische Anwendung bereitstellen, die anzeigt, wann eine Datensicherung beginnt und endet. Nutzer:innen könnten über diese Anwendung ggf. auch die Möglichkeit bekommen, einer Sicherung zum gegebenen Zeitpunkt zuzustimmen oder diese abzulehnen.

Benutzer:innenprofil-Roaming à la **LiMux-Projekt**

Im Rahmen der in Kapitel 1 erwähnten Machbarkeitsstudie 2020 [**vgl. Kapitel 1 / S. 7**] fand ein fachlicher Austausch mit [ehemaligen] Techniker:innen im LiMux-Projekt statt. Im Rahmen des LiMux-Projekts wurde ein Konzept für „Profilroaming der Benutzer:innen" unter Linux erarbeitet und erfolgreich erprobt.

Zusätzlich zur Unterscheidung von Arbeitsdaten und Profildaten wurde dort noch genauer innerhalb der Profildaten selbst unterschieden. Um Benutzer:innenprofile zu synchronisieren, ist es erforderlich eine Synchronisationsstrategie je Anwendung zu implementieren.

Bei der entfernten Ablage [Synchronisationsspeicherort] muss darauf geachtet werden, dass sich alle lokalen Dateieigenschaften [Rechte, Attribute] auf dem entfernten Speicherort abbilden lassen. Der Synchronisationsspeicherort könnte im Corporate-Netzwerk für die Endgeräte über eine SMB-Freigabe bereitgestellt werden, aber die Profilspeicherung selbst würde dann in über die SMB-Freigabe erreichbaren Linux-Dateisystem-Images erfolgen.

Die Profilsynchronisation sollte so wenig Arbeitseinschränkung wie möglich für die Anwender:innen bedeuten. Längere Wartezeiten sollten grafisch am Rechner [während An- und Abmeldung] visualisiert werden und sind grundsätzlich zu vermeiden. Die Anzeige von Synchronisationsfehlern oder -timeouts sollte für erfahrenere Anwender:innen optional zuschaltbar sein.

Herausforderungen bei vollwertigem **Profil-roaming der Benutzer:innen**

Die Herausforderung bei der Unterstützung von Mehrfachanmeldungen an verschiedenen Endgeräten gleichzeitig ist das Sicherstellen von konsistenten Benutzer:innenprofilen nach paralleler Offline-Nutzung an mehr als einem Gerät [möglichst ohne Eingriff seitens der Anwender:innen]. Wird ein Endgerät kontinuierlich von nur einer Person genutzt, dann findet die Profilsynchronisation im Alltag nur bei Abmeldung vom Arbeitsplatz statt. Während der Anmeldung wird lediglich abgeglichen, ob das serverseitige Profil neuer ist als das auf dem Arbeitsgerät. Meist ist das Profil auf dem Arbeitsgerät das aktuellere Profil.

DIE UNTERSTÜTZUNG VON MEHRFACHANMELDUNGEN AN VERSCHIEDENEN ENDGERÄTEN IN KOMBINATION MIT SERVERSEITIGEN PROFILEN, Z. B. IM KONTEXT FERNZUGANG, IST HERAUSFORDERND.

Bei der Anmeldung am Gerät sollte darauf geachtet werden, dass die Dauer der Profilsynchronisation begrenzt ist [maximale Profilladezeit]. Nur ein vollständig geladenes / synchronisiertes Profil sollte auch verwendet werden. Wechseln Anwender:innen auf ein anderes Gerät, werden die serverseitig gespeicherten Profildaten auf das neue Gerät synchronisiert [sofern keine zweite Anmeldung an einem anderen Gerät besteht]. Bei der Anmeldung muss sichergestellt werden, dass die Profilsynchronisation abgeschlossen ist, bevor die Komponenten der Arbeitsoberfläche gestartet werden.

Notebook-Anwender:innen melden sich meist nicht vom Arbeitsplatz ab, sondern versetzen ihr Gerät durch Schließen des Notebook-Deckels in den Standby-Modus. Hier muss überlegt werden, ob in z. B. wöchentlichen Intervallen eine Abmeldung vom Gerät erzwungen werden muss [um eine Synchronisation der Profildaten zum zentralen Profilspeicherort zu forcieren].

Für einzelne Anwendungen mag es sinnvoll sein, die Profildaten der jeweiligen Anwendung von der Synchronisation auszunehmen und dafür einen anwendungsinternen Mechanismus zur Datensynchronisation einzusetzen [z. B. Bookmark-Synchronisation in Webbrowsern].

Ferner ist zu betrachten, ob ggf. eine Profilsynchronisation auch außerhalb des Corporate-Netzwerks funktional sein muss. Als Möglichkeiten bieten sich Synchronisationsmechanismen an, die eine bestehende VPN-Verbindung nutzen oder sogar gänzlich unabhängig von VPN sind [d. h. basierend auf anderen Verschlüsselungsmechanismen wie z. B. SSH, https-Protokoll etc.].

Fazit Profilroaming der Benutzer:innen und Offline-Fähigkeit

Grundsätzlich wird die Profilsynchronisation und damit die Offline-Fähigkeit eines Linux-Arbeitsplatzes bzgl. der Daten der Benutzer:innen als machbar eingestuft. Die „Anforderung: Synchronisation der Benutzer:innenprofile" muss ggf. technisch auf ausgewählte Nutzungsszenarien eingeschränkt werden und dies dann organisatorisch [z. B. durch einschränkende Richtlinien] kompensiert werden. Die Implementierung einer vollständigen Synchronisation der Benutzer:innenprofile inklusive der Unterstützung von Profilroaming der Benutzer:innen sowie die damit einhergehenden Tests [und das Open-Source-Stellen des Konzepts und der zugehörigen Tools] sind als hochgradig zeitaufwendig einzustufen.

Konfigurationsmanagement und Softwareaktualisierungen

Das Konfigurationsmanagement erfolgt nur, wenn das Linux-Endgerät im Corporate-Netzwerk eingebucht ist. Ist das Endgerät **vollständig offline** oder verfügt es nur über **eingeschränkte Internetkonnektivität**, dann greifen die zuletzt im Corporate-Netzwerk auf das Endgerät übertragenen Einstellungen. Auch Compliance-Prüfungen, bezogen auf die zuletzt bekannte Konfiguration, bleiben im Hintergrund aktiv und schützen den Istzustand der Systemkonfiguration. Das Ausrollen von Sicherheitsupdates und das Nachinstallieren von Software [aus Softwarewarenkorb via Self-Service] ist prinzipiell denkbar [d.h. technisch möglich], auch für Phasen, in denen das Endgerät nur **eingeschränkte Internetkonnektivität** hat. Diese Funktionalität ist entsprechend der Sicherheitsrichtlinien des Corporate-Netzwerks ggf. einzuschränken.

Kritisch zu betrachten sind längerfristige Offline-Phasen. Hier wird ggf. das Gerät über einen längeren Zeitraum nicht mehr mit Sicherheitsupdates versorgt.

Offline-Fähigkeit von [ausgewählten] Fachverfahren

Inwiefern einzelne Fachverfahren für den Offline-Betrieb eines Endgeräts geeignet sind, ist vollständig abhängig von der Art der Fachanwendung sowie von der Bereitstellung.

Offline-fähig sind nur solche Fachverfahren, die nativ auf dem Endgerät ausgeführt werden können und die ausschließlich mit lokalen Arbeits- und Profildaten vollständig [bzw. weitestgehend] funktionsfähig sind. Bzgl. der Softwarearchitektur sind hier Qt- oder Java-basierte Anwendungen denkbar, sowie Windows-Anwendungen, die unter Wine betrieben werden können oder in einer lokalen Windows-Virtualisierung bereitgestellt werden. Solche Fachverfahrensbereitstellungen sind auch dann noch nutzbar, wenn das Endgerät **vollständig offline** ist oder nur über **eingeschränkte Internetkonnektivität** verfügt. Fachanwendungen in Offline-Phasen zu nutzen, wird voraussichtlich oft zu kombinieren sein mit organisatorischen Maßnahmen [z.B. Kopieren von Datenbeständen aus zentralen Gruppenordnern und Kommunikation an die Kolleg:innen, diese Daten bis zu einem späteren Zeitpunkt auf dem zentralen Speicherort nicht zu verändern].

DIE MÖGLICHKEIT DER OFFLINE-NUTZUNG EINES FACHVERFAHREN MUSS GEPRÜFT UND VERSCHIEDENE LÖSUNGSWEGE ANALYSIERT WERDEN.

Eine weitere Möglichkeit, Fachanwendungen zu nutzen, während man nicht mit dem Endgerät im Corporate-Netzwerk eingebucht ist, ist eine Bereitstellung des Fachverfahrens über eine Web-Applikation, die auch außerhalb des Behördennetzwerks noch erreichbar ist. Solche Verfahrensplattformen müssen ausreichend vor Fremdzugriff geschützt werden [z.B. mind. mittels 2-Faktor-Authentifizierung].

LINUX-STUDIE **THEMEN IM DETAIL**

THEMA 3

Systemmanagement

Eine sehr wichtige Anforderung an einen Enterprise-Arbeitsplatz ist die zentrale Verwaltbarkeit des Arbeitsplatzes [d. h. aller ca. 25.000 IT-Arbeitsplätze im Land SH] mit gut bedienbaren Systemmanagement-Tools.

Im Bereich Systemmanagement unterscheiden wir folgende Bereiche:

- Vollautomatisierte Installation von Endgeräten **[OSD]**, ausführbar durch Dritte [externe Dienstleister:innen] ohne personelle Interaktion auf Dataport-Seite
- Konfigurationsmanagement der Endgeräte im laufenden Betrieb **[KM]**
- Softwareverteilung und Patch-Management **[SWD + PM]**
- Inventarisierung und Berichtswesen **[INV+LOG]**

Ergänzend sollen die o. g. **Systemmanagement-Komponenten durch ein Life-Cycle-Management [LCM] visualisiert und „bedienbarer"**[13] gemacht werden.

Eine regionale Herausforderung bzgl. des Systemmanagements ist die sehr starke Untergliederung des schleswig-holsteinischen Landesnetzes in viele unterschiedliche Standorte.

Life-Cycle-Management-Frontend

Zeitnah steht im Linux-Arbeitsplatz-Projekt die Auswahl des LCM-Frontend-Produkts an.
Insbesondere übernimmt das LCM-Produkt, neben der grafischen Aufbereitung der Systemmanagement-Aufgaben im Webbrowser, die Funktion der Versorgung der dezentralen Standorte über sogenannte **Satelliten-Systeme**.[14]

In technischen Vorbetrachtungen wurde die Software TheForeman [Open-Source-Variante des Produkts „Red Hat Satellite 6"] getestet. TheForeman wurde bereits für andere Projekte bei Dataport erfolgreich eingesetzt. Das Produkt Uyuni [Open-Source-Variante des Produkts „SUSE Manager"] ist in Form des SUSE Managers im Dataport-Rechenzentrum ebenfalls bekannt. Weitere Produkte wurden bislang noch nicht näher betrachtet, dies muss im Rahmen einer gründlichen Markterkundung noch erfolgen. Das LCM-Produkt muss mindestens die zum Einsatz kommen werdende Linux-Distribution unterstützen [Auswahlprozess steht noch aus, **vgl. Kapitel 7 / S. 71**]. Unterstützung für weitere Linux-Distributionen ist wünschenswert [**vgl. S. 25, Multi-Vendor-Strategie**].

Motivation einer generischen Konzeptionierung des Systemmanagements ist die Vermeidung von zu starken Abhängigkeiten zwischen der eingesetzten GNU-/Linux-Distribution und den Softwarekomponenten des Systemmanagements [insbesondere des LCM-Frontends]. Nachteil einer generischen Lösung im Bereich des Systemmanagements ist eine längere Vorlaufzeit, bevor eine flächendeckende Bereitstellung der Linux-Arbeitsplätze erfolgen kann. Die Bereitstellung des LCM-Frontends und der zugehörigen Satelliten-Systeme wird bzgl. des initialen Server-Rollouts als sehr kostenintensiv bewertet, wodurch die Produktwahl sehr sorgfältig getroffen werden muss, insbesondere im Hinblick auf eine langfristige, nachhaltige und erweiterbare Nutzbarkeit des gewählten LCM-Frontend-Produkts.

Betriebssysteminstallation

Anforderung für die Betriebssysteminstallation im Enterprise-Umfeld ist eine vollautomatisierte Installation von Endgeräten [OSD], ggf. ausführbar durch Dritte [externe Dienstleister:innen] ohne personelle Interaktion auf Dataport-Seite.

Das OSD-Produkt für die Linux-Arbeitsplatz-Modelllinie wird distributionsspezifisch auszuwählen sein. Eine bereits vorhandene Integration in das LCM-Frontend ist wünschenswert, aber nicht zwingend [weil die betrachteten LCM-Produkte modular erweiterbar sind]. **Die Installationsautomatisierung gängiger Enterprise- und Community-Distributionen wird nativ von den bisher betrachteten LCM-Produkten [TheForeman und SUSE Manager] bereits unterstützt.**[15]

Konfigurationsmanagement

Eine hochskalierte Automatisierung des Konfigurationsmanagements [inklusive Remote Execution] von Linux-Systemen [unabhängig, ob Server oder Desktop] ist machbar und im Praxisbetrieb seit Langem erprobt. Es gibt mehrere ähnlich wertige Systemmanagement-Tools, mit denen eine Umsetzung erfolgen kann. Welches der Tools [Ansible, Puppet, SaltStack etc.] für die Konfigurationsverwaltung der Linux-Arbeitsplatz-Modelllinie bei Dataport zum Einsatz kommen wird, ist noch nicht final festgelegt. Die Wahl des einzusetzenden KM-Produkts kann nicht autark erfolgen, sondern ist gekoppelt an die Produktwahl des LCM-Frontends.

Softwareinstallation und **Patch-Management**

Die Basissoftware des Linux-Arbeitsplatzes für die Landesverwaltung Schleswig-Holstein wird über die Paketarchive der Distribution [bzw. lokale Paketspiegel] und über Paketarchive von Drittanbietern [inklusive On-Premises-Paketarchiv, s. u.] installiert. Die Anzahl der Pakete, die über Drittanbieter-Paketarchive [bzw. lokale Spiegel selbiger] ergänzt werden müssen, soll nach Möglichkeit niedrig gehalten werden.

Patch-Management [PM] bezogen auf GNU-/Linux-Distribution muss als Paket- bzw. Software-Update-Management verstanden werden, d. h., das Patch-Management ist eng verzahnt mit der Softwareverteilung [anders als bei Windows-Systemen]. Normalerweise erfolgt die Bereitstellung von Paket-Updates im Sinne des Patch-Managements durch den Linux-Distributor. Das Einziehen einer Qualitätssicherungsebene durch das Bereitstellen von Paketspiegeln und der Implementierung von Auditierungsverfahren wird benötigt. Die LCM-Frontends TheForeman [Plugin Katello] und Uyuni [bzw. SUSE Manager] bieten hierfür gut bedienbare Oberflächen, mit denen Softwareupdates vor der Freigabe zum Ausrollen geprüft werden können.

Systemanpassungen wie Desktop Branding, Deaktivierung bestimmter Desktop-Funktionen, Ausrollen von kundenspezifischen Standardeinstellungen etc. werden über eigens entwickelte

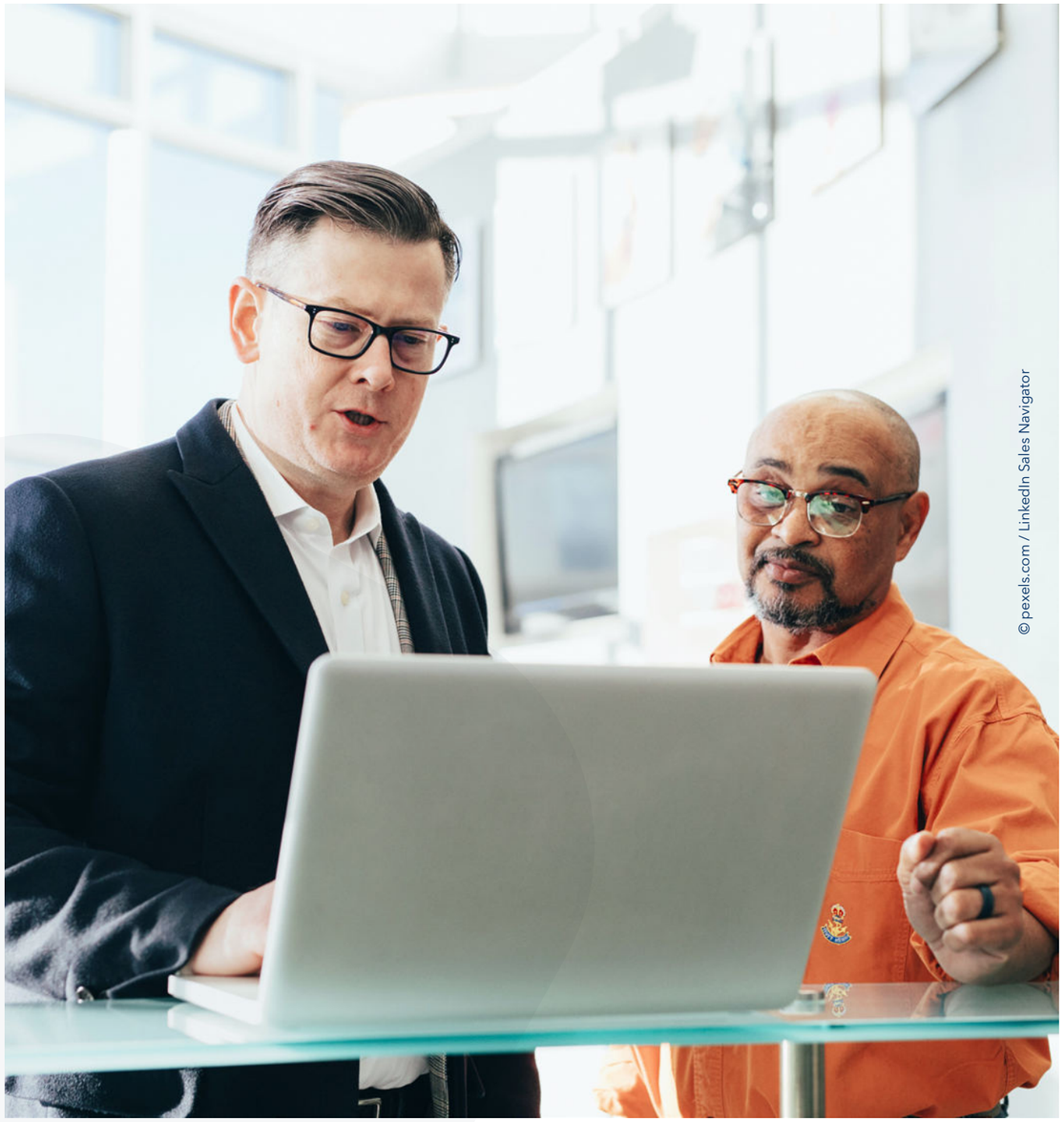
Fortsetzung ▸

[13] Systemmanagement-Komponenten
Grundsätzlich lassen sich alle Komponenten des Systemmanagements sehr gut ohne LCM-Frontend administrieren. Erwartung an ein LCM-Frontend ist die Vereinfachung von Bedienprozessen und das Abflachen notwendiger Lernkurven beim Personal, um die zentrale Administration der Linux-Arbeitsplätze bedienen zu können.

[14] Satelliten-Systeme
Diese Satelliten sind Infrastruktur-Server in den [entlegenen] Verwaltungsstandorten, die lokal vor Ort die Funktionen des Systemmanagements bereitstellen, aber zentral von einer LCM-Hauptinstanz [fern-]gesteuert und bzgl. des Berichtswesens abgefragt werden können.

[15] Für die Bereitstellung eines SUSE-Linux-Enterprise-Desktop-Systems wurde AutoYAST erfolgreich getestet. In SUSE Manager existiert seit 2020 die Funktion SaltBoot als Alternative zu AutoYAST.

LINUX-STUDIE **THEMEN IM DETAIL**



© pexels.com / LinkedIn Sales Navigator

Overlay-Pakete provisioniert, um eine Überfrachtung der KM-Konfiguration zu vermeiden.
Der Linux-Arbeitsplatz wird einige wenige Pakete aus On-Premises-Paketarchiven benötigen. Hierbei wird es sich manchmal um die schnelle Bereitstellung von Updates und Backports, aber auch um die Bereitstellung eigener Pakete [wie z.B. das Paket für Desktop Branding] handeln. Die hierfür benötigten Entwicklungsabläufe und -werkzeuge [Git Code Repository, Source Code Review Workflows, Continuous Integration, Software-/Paket-Release-Management] werden im Rahmen des Linux-Arbeitsplatz-Projekts bei Dataport konzeptioniert werden und stehen später ggf. auch anderen Projekten langfristig zur Verfügung.

Oberste Priorität bzgl. des Patch-Managements wird sein, das Delta [d.h. die Anzahl und Größe der Unterschiede] zwischen den Paketen der Distribution und den selbst bereitgestellten Paketen so klein wie möglich zu halten. Hierfür muss eine Zusammenarbeit mit dem Distributor möglich sein.

Berichterstattung
Inventarisierung und Protokollierung

Die Möglichkeiten des Reportings sollen sich an der aktuell im Land SH betriebenen Windows-Arbeitsplatz-Modelllinie orientieren. Aktuell werden in regelmäßigen Intervallen verschiedenste Berichte angefragt und erstellt [sogenanntes ActiveDirectory-Reporting].

Alle Linux-Arbeitsplätze, wie auch bei der Windows-Produktlinie in Schleswig-Holstein, sollen über ein zentrales Tool bzgl. Hardware-Ausstattung und Softwarezusammenstellung inventarisiert werden [Produktauswahl steht noch aus, ggf. Teilkomponente des LCM-Frontends].

THEMA 4

Backend Microsoft
Infrastruktur Parallelbetrieb

Für den Migrationszeitraum [**Windows-Arbeitsplatz ▸ Linux-Arbeitsplatz**] wird mit einem Parallelbetrieb beider Betriebssysteme gerechnet. Alternative Bereitstellungsmethoden von Fachanwendungen werden ggf. sehr langfristig einen solchen Parallelbetrieb erfordern.

Auf eine gute Interoperabilität von Arbeitsplätzen beider Produktlinien [MS Windows, GNU/Linux] im gleichen Netz bzw. in benachbarten Netzen [VLANs] wird während der Migration ein deutlicher Fokus liegen. Insbesondere für einen Mischbetrieb mehrerer Betriebssysteme ist eine übergreifende Identitätsverwaltung für beide Modelllinien immens wichtig. Hier stellt **Active Directory** [16] eine gute technische Lösung dar. Ähnliches gilt für die Bereitstellung eines gemeinsamen Storage-Backends. Für einen Übergangszeitraum müssen die Arbeitsplätze beider Modelllinien auf eine gemeinsame Dateiablage zugreifen können.

Identitätsmanagement

Im ersten Ansatz ist mittelfristig die Anbindung der Linux-Arbeitsplatz-Modelllinie an den bereits vorhandenen Verzeichnisdienst, das Microsoft Active-Directory der Landes-IT-Infrastruktur, angedacht. Als langfristige Zielvision wird auch bzgl. der Server-Backend-Komponenten [z.B. Identitätsmanagement, Storage-Bereitstellung im Intranet etc.] eine Ausrichtung hin zu [mehr] Open Source betrachtet.

Ausschlaggebend für die technische Implementierung der Active Directory Integration unter Linux wird die Konfigurationsempfehlung der eingesetzten Linux-Distribution sein. Die Anbindung des Linux-Arbeitsplatzes an den Landesverzeichnisdienst wird so umgesetzt werden, dass der Client vollständig Kerberos-fähig sein wird und dadurch bzgl. Single Sign-On [auch via Webbrowser] ähnlich aufgestellt sein wird wie Arbeitsplätze der Windows-Modelllinie.

Technisch ist via Active Directory die Bereitstellung von Linux-Benutzer:innenkonten [d.h. POSIX-Konten und -Gruppen] für Linux-Arbeitsplätze möglich. Dies wird auf der Seite des Windows Active Directory über die zusätzliche Windows-Server-Dienstrolle „Identitätsverwaltung für UNIX-Komponenten" als Funktionalität bereitgestellt; auf der Linux-Seite wird voraussichtlich der Dienst „SSSD" [System Security Services Daemon] zum Einsatz kommen und die im Active Directory konfigurierten Benutzer:innenkonten [und -gruppen] transparent und offline-fähig auf dem Linux-Arbeitsplatz bereitstellen [**vgl. S. 46**].

Die Windows-spezifische Konfiguration von Arbeitsplatz und Benutzer:innenprofil via MS-AD-Gruppenrichtlinien wird unter Linux nicht 1:1 abbildbar sein. Die Funktionen des Gruppenrichtlinien-Deployments werden in den Bereich des Systemmanagements [**vgl. Kapitel 5/Thema 2**] verlagert werden. Bestehende Regelwerke müssen individuell angepasst werden bzw. vollständig neu und ausgerichtet auf den Konfigurationsstil von Linux-Systemen konzipiert werden [insbesondere benutzer:innenspezifische Gruppenrichtlinien-ACLs werden sich nicht ohne Weiteres im Konfigurationsmanagement abbilden lassen].

[16] Active Directory
ist aktuell in zwei Implementierungen verfügbar: Windows Active Directory [proprietäres Produkt, MS Windows Server] und Samba Active Directory [Open-Source-Software, installierbar auf GNU/Linux und BSD-ähnlichen Server-Plattformen].

Netzwerk-Infrastruktur

Eine besondere Herausforderung wird ein Redesign der Netzwerk-Infrastruktur im Landesnetz von Schleswig-Holstein sein. Der Geräte-Rollout der Linux-Arbeitsplätze wird voraussichtlich nicht im Netzwerksegment der Windows-Modelllinie [hier wird aktuell Microsoft SCCM genutzt] möglich sein. Eine Bereitstellung muss evtl. über separate VLANs/Subnets in den Behörden-Örtlichkeiten erfolgen. Für das Management der verschiedenen Netzsegmente wird aktuell bei Dataport der Einsatz der **Software Infoblox** [17] [insbesondere zur Bereitstellung einer zentralen DHCP-Datenbank] vorbereitet.

Storage-Backend

Von dem Begriffskonzept des „Benutzer:innenlaufwerks" muss im Linux-Umfeld Abstand genommen werden, da es unter Linux keine sogenannten Laufwerksbuchstaben gibt. Der Zugriff auf als SMB-Freigaben bereitgestellte „Benutzer:innenlaufwerke" ist möglich und wird via grafischer GUI-Dialoge von den meisten Dateibrowsern unter Linux als Feature bereitgestellt [z.B. im Nautilus-Dateibrowser des GNOME-Desktops via **GVFS** [18]]. Ebenfalls ist ein automatisches Einbinden [Mounten] von SMB-Freigaben mittels eines Automounters [autofs] möglich.

Eine Linux-Client-Anbindung an Workfolders für MS Windows wird serverseitig von den aktuell verfügbaren Microsoft-Windows-Server-Versionen nicht unterstützt. Eine ähnliche Implementierung [Dateisynchronisation via https] ist mittels anderer Storage-Backend-Produkte [Seafile, Nextcloud, SyncThing etc.] möglich [**vgl. S. 46**].

Zugriff auf Gruppenablage-Ordner, die als SMB-Freigabe [oder auch als DFS-Namespaces] im Netz bereitgestellt werden, ist von GNU-/Linux-Systemen aus möglich. Vorteilhaft beim Arbeiten auf Gruppenordnern via SMB-/CIFS-Protokoll ist die im Protokoll implementierte Möglichkeit des „File-Lockings". Dateien, die für die Bearbeitung geöffnet sind, werden gegen Schreibzugriff durch andere Benutzer:innen derselben Gruppe geschützt.

Die Anzeige und das Ändern von ACLs auf dem Linux-Client sind allerdings problematisch, wenn das Fileserver-Backend der SMB-Freigabe ein MS-Windows-System ist. [19]

Aktuell erfolgt die Gruppenablage in den jeweiligen Verwaltungen in Schleswig-Holstein je nach Ressort entweder auf eigenen Standort-Servern oder zentral bei Dataport. Aktuelle Planungen für den IT-Strukturwandel in Schleswig-Holstein gehen in Richtung eines vollständig zentral verwalteten IT-Systems, bereitgestellt durch Dataport. Im Rahmen solcher Umstellungsprozesse wird es zu Migrationen von Storage-Servern und dabei auch zu einer Evaluierung möglicher alternativer [Open-Source] Storage-Backends kommen [**z. B. Samba** [20]].

Druckdienste

Die Integration des Linux-Arbeitsplatzes in eine Microsoft-Windows-Druckumgebung ist mit mittlerem Aufwand technisch realisierbar. Voraussetzung ist eine ordnungsgemäße Integration des Linux-Arbeitsplatzes in den Active-Directory-Verzeichnisdienst. Deutlich einfacher hingegen ist die direkte Anbindung von Linux-Arbeitsplätzen an einen zentralen **CUPS-Server** [21].

Auch für einen Linux-Windows-Mischbetrieb ist die Bereitstellung eines Nicht-Microsoft-Druckdienste-Backends mittels CUPS und Samba die technisch leichter wartbare Lösung.

Linux-Arbeitsplätze können in einem solchen Set-up direkt an einen zentralen CUPS-Server drucken. Windows-Arbeitsplätze senden ihre Druckjobs zu einem auf dem CUPS-Server laufenden Samba-Dienst und dieser reicht die Druckjobs dann weiter an den CUPS-Dienst des Systems. Kommt es im Rahmen des IT-Strukturwandels in Schleswig-Holstein zu einer zentraleren Ausrichtung der Druckdienst-Umgebungen, wird eine Open-Source-Drucklösung als Alternative zu einem Windows-Druckdienst in Betracht gezogen werden.

Ferner ist die Härtung des CUPS-Dienstes auf dem lokalen Linux-Arbeitsplatz selbst wichtig. Dieser ist je nach Distribution in seiner Standardkonfiguration zu offen konfiguriert.

Bei einigen Druckgeräten wird es zu Einschränkungen kommen. Z.B. fehlt vielen gängigen Multifunktionsdruckermodellen bzgl. der Funktionen, die über das Drucken hinausgehen, je nach Hersteller und dessen Linux-Affinität, eine ausreichende Linux-Unterstützung. User Interfaces [UI] für den vollständigen Funktionsumfang eines Multifunktionsdruckers müssen in der Regel von dem:der Hersteller:in bereitgestellt werden und kommen daher im Linux-Kontext eher selten vor. Die Funktionen von Multifunktionsdruckern werden, wenn unterstützt, als Einzelanwendungen eingerichtet und verwendet. ●

[17] Software Infoblox
www.infoblox.com

[18] GVFS
GNOME Virtual File System

[19] ACLs
Die Open-Source-Software Samba hingegen ist bereits optimal für die Bereitstellung von SMB-Freigaben für Linux-Clients ausgelegt.

[20] Samba
www.samba.org

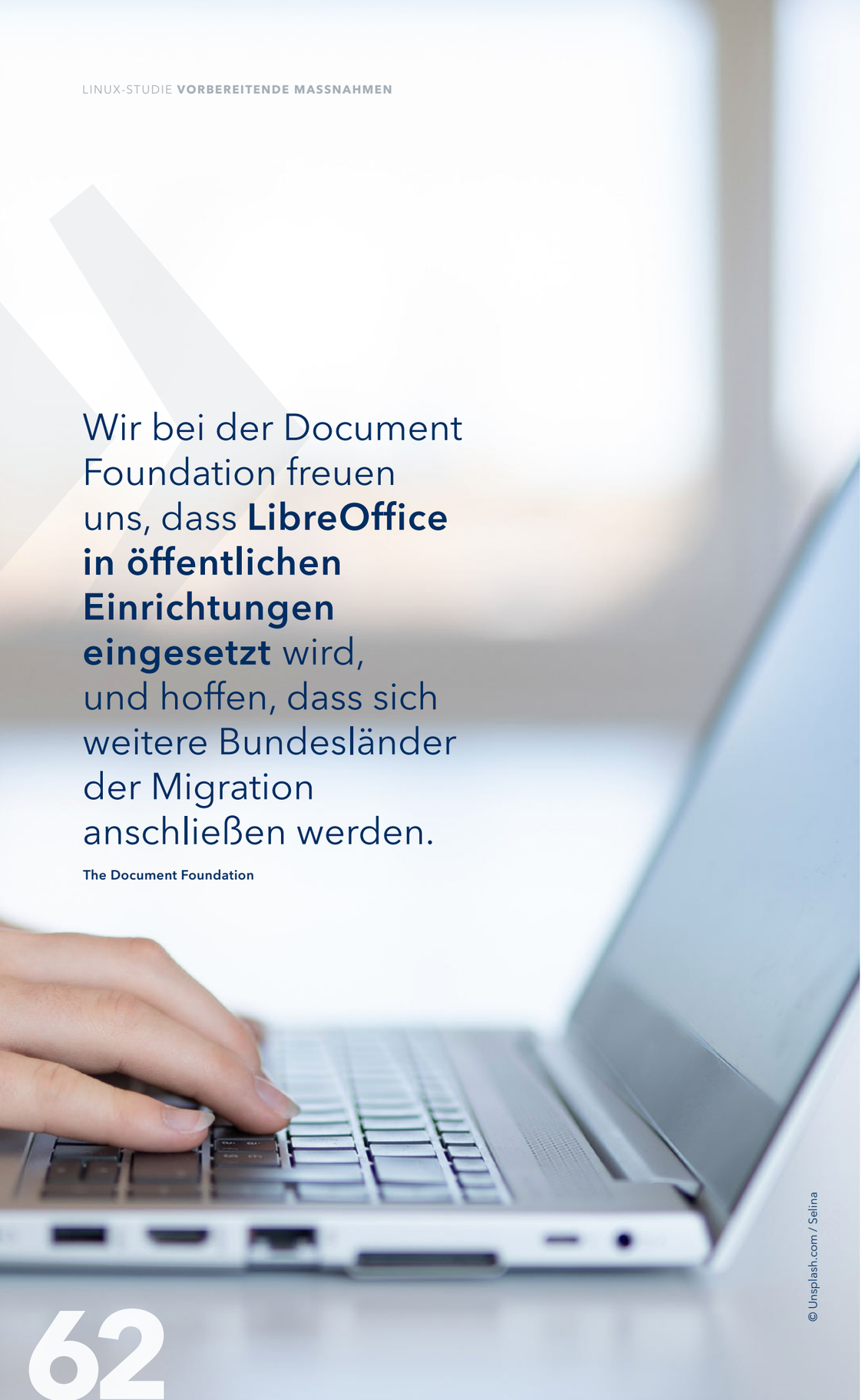
[21] CUPS
Common Unix Printing System
www.cups.org

6

Vorbereitende **Maßnahmen**

Wir bei der Document Foundation freuen uns, dass **LibreOffice in öffentlichen Einrichtungen eingesetzt** wird, und hoffen, dass sich weitere Bundesländer der Migration anschließen werden.

The Document Foundation



© Unsplash.com / Selina

LINUX-STUDIE **VORBEREITENDE MASSNAHMEN**

Vorbereitende **Maßnahmen**

Für Anwender:innen beinhaltet jede größere IT-Umstellung eine Vielzahl an kleineren und größeren Umgewöhnungsprozessen am eigenen Arbeitsplatz.

Im Rahmen „vorbereitender Maßnahmen" sollen diese verschiedenen Umgewöhnungsprozesse in kleinere und zeitlich versetzt ausrollbare Schritte aufgeteilt werden, sodass die Umstellung des Betriebssystems schließlich nur noch ein „kleiner" Schritt zu einer Open-Source-basierten IT-Landschaft in der Landesverwaltung Schleswig-Holstein darstellt.

Innerhalb einer, vornehmlich aus Microsoft-Produkten aufgebauten, IT-Infrastruktur können die folgenden vorbereitenden Maßnahmen getroffen werden, um den Anwender:innen den Umstieg auf das Endgeräte-Betriebssystem Linux zu erleichtern.

Die aktuelle Vision für die IT-Infrastruktur der Landesverwaltung Schleswig-Holstein sieht eine Architektur vor, die einen weitestgehend plattformunabhängigen Arbeitsplatzbetrieb ermöglichen wird. Fachverfahren, Kollaborations-Software etc. werden langfristig als Webapplikationen bereitgestellt und sind dann unabhängig vom Betriebssystem des Endgeräts nutzbar. Eine zeitgemäße IT-Infrastruktur bietet die Möglichkeit, einen Mischbetrieb verschiedener Endgerät-Betriebssysteme abbilden zu können.

Das Endgerät der Anwender:innen wird mit einem minimalen Grundstock an Basis-Anwendungen ausgestattet sein. Bei der Auswahl dieser Basissoftware wird auf Open-Source-Standards sowie auf eine plattformübergreifende Bereitstellbarkeit der verschiedenen Softwarekomponenten geachtet.

Umstellung auf **offene Dokumentenformate**

Das Bürokommunikationsprodukt Office von Microsoft ist unter Linux nicht nativ einsetzbar. Somit impliziert die Umstellung auf einen Linux-Arbeitsplatz eine Softwareumstellung im Bereich der Bürokommunikation. Ein Großteil des produktiven Arbeitens in der Verwaltung ist das Erstellen von Office-Dokumenten [Texte, Tabellen etc.].

Als vorbereitende Maßnahme wird das Speicherformat in allen Behörden auf das OpenDocument-Dateiformat umgestellt. Vorhandene Dokumente verbleiben weiterhin im OpenOffice-XML-Format. Neue Dokumente werden zukünftig im OpenDocument-Format gespeichert.

Die Umstellung auf ein offenes Office-Speicherformat ist ein wichtiger Schritt zur digitalen Souveränität, unabhängig vom Office-Paket und dem eingesetzten Betriebssystem.

Umstellung auf plattformübergreifende **Open-Source-Produkte**

Die Vielfalt der Software auf dem Arbeitsplatzsystem gilt es zu minimieren, die verbleibenden Grundbausteine werden sein: Büroarbeit und -kommunikation, Zugriff auf Webseiten im Internet, Programm für Dateisynchronisation sowie verschiedene Hilfsanwendungen [Taschenrechner, Farbauswahlpipette, Bildschirmkopie erstellen etc.].

Die Auswahl einer neuen Arbeitsplatzsoftware [z. B. Internetbrowser, Zeichenprogramm, Kennwortverwaltung etc.] orientierte sich bislang an der optimalen Bereitstellbarkeit einer gewünschten Funktionalität unter dem genutzten Betriebssystem [d. h. zum aktuellen Zeitpunkt: unter Microsoft Windows].

Zukünftig werden zwei zusätzliche Aspekte betrachtet:

- **Ist die Software plattformübergreifend[22] konzipiert und wird sie für mehrere Zielarchitekturen entwickelt? Ist die Software für verschiedene Betriebssysteme erhältlich?**
- **Ist die betrachtete Software ein Open-Source-Produkt oder eine proprietäre Anwendung?**

Als vorbereitende Maßnahme wird die Softwarelandschaft in der Landesverwaltung Schleswig-Holstein schrittweise, gemäß dieser Zielvorgaben, angepasst werden.

[22] Plattformübergreifende Softwarearchitekturen

erlauben es, eine so konzipierte Software unter mehr als einem Betriebssystem zu betreiben. Hierfür muss der Quellcode der Software so ausgelegt sein, dass er sich für verschiedene Zielplattformen [Betriebssysteme] übersetzen lässt und dass dabei ein auf der Zielplattform verwendbares Programm daraus entsteht.

Umstellung des Standardbrowsers

Der zurzeit als Standardbrowser unter Windows 10 definierte Microsoft Edge [basierend auf Chromium] steht seit Q3 2020 als Linux-Variante zur Verfügung, allerdings nicht als Open-Source-Software. Open-Source-Alternativen sind beispielsweise Mozilla Firefox und Chromium. Beide Produkte werden plattformübergreifend entwickelt.

Auf Windows-Arbeitsplätzen in Schleswig-Holstein steht Mozilla Firefox bereits seit einiger Zeit als Installationspaket alternativ zur Verfügung, ist aber nicht der Standardbrowser.

Bei der Definition eines neuen, plattformübergreifend verfügbaren Open-Source-Standardbrowsers zeichnet sich aktuell die Präferenz für einen Chromium-basierenden Browser ab [insbesondere aufgrund der Kompatibilität zu gängigen Open-Source-Videokonferenzprodukten].

In jedem Fall erfordert die Definition eines neuen Standardbrowsers ein ausgiebiges Testen vorhandener Webanwendungen auf Kompatibilität. Hierbei wird auf plattformübergreifende Testschemata geachtet: Alle Tests werden von den unterschiedlichen zum Einsatz kommenden Arbeitsplatz-Betriebssystemen aus durchgeführt werden.

Die Festlegung auf einen Open-Source-Standardbrowser soll nach aktueller Planung bereits unter Windows erfolgen. Bleibt den Anwender:innen der Standardbrowser bei der Umstellung des Betriebssystems erhalten, sollten die meisten webbasierten Fachverfahren ohne weitere Anpassungen funktionieren.

Umstellung auf LibreOffice

Das Produkt MS Office ist keine Open-Source-Software und eine Installation unter Linux wird nicht nativ unterstützt. Die meisten Linux-Distributionen bieten verschiedene Office-Pakete an. LibreOffice ist dabei das am weitesten entwickelte Produkt und wird plattformübergreifend [d. h. auch für Windows] von den LibreOffice-Entwickler:innen bereitgestellt.

Als vorbereitende Maßnahme wird die Umstellung auf LibreOffice bereits auf den Windows-Arbeitsplätzen erfolgen. Bei einer anschließenden Linux-Arbeitsplatz-Migration liegen die Dokumente bereits in einem kompatiblen Speicherformat vor und die Anwender:innen sind für das Arbeiten mit LibreOffice bereits geschult.

Zentrale Infrastruktur [Plattformunabhängigkeit]

Vorbereitende Maßnahmen im Bereich der zentralen Infrastruktur sind:

- **Portierungen von Software, die nach einer Umstellung auf Linux dem Funktionserhalt [insbesondere im Bereich der Fachverfahren] dienen**
- **Neueinführung von alternativen Werkzeugen für Kommunikation und Kollaboration**

Kollaborationsplattformen

Als zukünftige Plattform zur Zusammenarbeit ist der Einsatz der Online-Kollaborationsplattform dPhoenixSuite angedacht. Bis zu dessen Bereitstellung soll „Outlook on the Web" verwendet werden. Als Webapplikation werden beide Dienste auf der Linux-Arbeitsplatz-Modelllinie ohne weitere Maßnahmen sofort einsetzbar sein.

Benutzer:innendaten

Benutzer:innendaten von Windows-Anwender:innen werden zurzeit in Windows-Arbeitsordnern gespeichert. Diese sind nicht mit Linux kompatibel. Eine plattformunabhängige Lösung wird bereits auf den Windows-Arbeitsplätzen bereitgestellt werden. Bei einem Umstieg auf Linux werden die Daten dann bereits kompatibel zu Linux abgelegt und verfügbar sein.

Fachanwendungen

Viele Fachverfahren sind reine Windows-Anwendungen, die nicht unter Linux eingesetzt werden können. Bereits bestehende Fachanwendungen können über alternative Bereitstellungsmethoden auf dem Linux-Arbeitsplatz genutzt werden. Den Ressorts der Landesverwaltung Schleswig-Holsteins wird empfohlen, bei zukünftigen Ausschreibungen plattformübergreifende [z.B. Implementierungen in Java, Qt] oder plattformunabhängige [d.h. webbasierte] Entwicklung als Anforderung zu formulieren. Neue Fachanwendungen sollten nicht nur das Office-Open-XML-Format, sondern auch das Open-Document-Format im- und exportieren können. Neue Fachverfahren sollen in Schleswig-Holstein bevorzugt als Open-Source-Software entwickelt und unter eine passende Lizenz gestellt werden.

Druckdienste

Die Standardsoftware unter Linux für die Ansteuerung von Drucker-Hardware ist das „Common Unix Printing System" [CUPS]. Die Druckdienste der bestehenden Druckinfrastrukturlösung müssen im Detail auf CUPS-Kompatibilität geprüft und ggf. angepasst werden. Druckdienste im Behördennetzwerk müssen über CUPS vom Linux-Arbeitsplatz aus ansteuerbar sein [insbesondere via IPP-Protokoll]. Langfristig wird die Umstellung der proprietären Druckinfrastruktur im Land Schleswig-Holstein auf das ebenfalls für Druck-Server geeignete Open-Source-Drucksystem CUPS empfohlen.

Identitätsmanagement

Im ersten Prototypen des Linux-Arbeitsplatzes werden sich Anwender:innen bei der Anmeldung am Linux-Arbeitsplatz gegen das bestehende, via Microsoft Active Directory bereitgestellte Identitätsmanagementsystem [IAM] authentifizieren. Die Pflege von Benutzer:innen- und Computerkonten erfolgt somit mittelfristig weiterhin in der bestehenden IAM-Lösung. Ein langfristiger Umstieg auf ein Open-Source-IDM-System befindet sich zum aktuellen Zeitpunkt in der Analysephase.

Somit ist mittelfristig eine Anbindung der Linux-Arbeitsplätze an die Windows-Anmeldedienste erforderlich. Das produktiv genutzte Active Directory der Landesverwaltung muss für die Einbindung von Unix-ähnlichen Arbeitsplätzen und für die Bereitstellung von POSIX-konformen Benutzer:innenkonten vorbereitet werden [insbesondere durch eine LDAP-Schema-Erweiterung]. Für die automatisierte Betriebssysteminstallation [OSD] muss eine Schnittstelle zum Active Directory erarbeitet werden, mit der automatisiert Computerkonten für Linux-Arbeitsplätze angelegt werden können.

Für die Entwicklungsphase der Linux-Arbeitsplatz-Modelllinie muss bzgl. Identitätsmanagement eine der Produktivumgebung möglichst ähnliche Test-Infrastruktur bereitgestellt werden. Linux-Arbeitsplatz-spezifische Anpassungen an der Testumgebung müssen ausführlich dokumentiert und mit den Infrastrukturteams bei Dataport abgestimmt werden.

Mit den involvierten Teams muss ebenfalls eine Roadmap festgelegt werden, ab wann die ersten Linux-Arbeitsplätze in das produktiv betriebene Active Directory integriert werden können bzw. sollen. Insbesondere muss für die entwickelten Verfahren und Schnittstellen festgelegt werden, in welcher Weise und in welcher Projektphase diese in die bestehende Infrastruktur übertragen werden können. ●

Die **digitale Souveränität des Staates sichern:** Das heißt auch, Abhängigkeiten von einzelnen Hersteller:innen zu vermeiden. Dataport tut das. Mit dPhoenixSuite haben wir einen Arbeitsplatz entwickelt, der das ermöglicht. **Mit Open-Source-Lösungen.**

Dataport AöR

LINUX-STUDIE **VORBEREITENDE MASSNAHMEN**

© pexels.com / Fauxels

Personal und Organisation

Personalentwicklung

Für die Verwaltung, Entwicklung, Fortschreibung und den Betrieb einer Linux-Modelllinie sind unterschiedliche Tätigkeiten notwendig. Dabei werden Tätigkeitsbereiche bzw. Aufgabengebiete in der Verwaltung in Form von Stellenbeschreibungen festgeschrieben. Üblicherweise liegen diesen Stellenbeschreibungen definierte Rollenbeschreibungen zugrunde, aus denen Stellenbeschreibungen abgeleitet werden.

Genau diese Rollen- und Stellenbeschreibungen sind bei der Entwicklung einer neuen Modelllinie näher zu betrachten, inhaltlich zu prüfen und zu ergänzen. Sehr wahrscheinlich ist für die neue bzw. geänderte Aufgabenerledigung auch neues Wissen erforderlich. Diese Erkenntnisse sind zu berücksichtigen bei der Aktualisierung der Stellenbeschreibungen und den Rollenbeschreibungen. Die Beschreibungen dienen der Fortentwicklung des vorhandenen Personals [Personalentwicklung], aber stellen auch die Grundlage für Personalveränderungen dar und werden z. B. für interne und externe Stellenausschreibungen genutzt.

Organisationsanpassung

Mit einer neuen Modelllinie wird wahrscheinlich eine Organisationsanpassung einhergehen. Bei Migrationsprojekten über mehrere Jahre sind hier verschiedene Szenarien denkbar. Üblicherweise erfolgen während der Laufzeit des Projektes viele operative Aufgaben aus dem Projekt heraus. Wichtig ist, bereits innerhalb des Projektes frühzeitig die Überführung in die Linie [Transition Management] vorzubereiten, um einen nahtlosen Übergang in den Regelbetrieb sicherzustellen.

Eine besondere Herausforderung stellen das Personalwachstum bzw. eine zu erwartende Personalverschiebung am Ende der Entwicklungsphase dar, wenn die Modelllinie in höherer Stückzahl dem:der Kund:in zur Verfügung gestellt wird. Zu diesem Zeitpunkt muss bereits eine Organisationsstruktur vorhanden sein, über die ein schneller Anstieg an Personalbedarf effektiv und kurzfristig abgewickelt werden kann.

Bei der Entwicklung einer neuen Modelllinie auf Basis von Open-Source-Software kann man von einem Paradigmenwechsel sprechen. Im Kontext einer Organisationsanpassung prägt sich dieser an unterschiedlichen Stellen aus. Es werden neue Rollen innerhalb des Unternehmens erforderlich sein, um die Wertschöpfung von Open Source voll nutzen zu können. Oft gestalten sich diese Rollen in Form eines OSS-Community-Managements oder erweiterten Partner:innenmanagements aus. Ein weiterer wichtiger Baustein ist die feste Etablierung einer OSS-Strategie im Unternehmen, um Richtlinien und abgestimmte Vorgehensweisen im Detail zu entwickeln. Dies ist für die Compliance, also die Einhaltung rechtlicher Vorgaben, ein MUSS-Kriterium. Schließlich wird durch die Implementierung von Änderungen bestimmter Prozesse auch eine Anpassung der bestehenden Prozess-Landkarte erforderlich sein. Das ggf. neue Vorgehen ist stimmig in den vorhandenen Product-Life-Cycle und auch in das Gesamtunternehmen einzugliedern.

Schulungen [Trainings] & Zertifizierungsprogramme

Für ein Unternehmen stellt es eine Herausforderung dar, zum benötigten Zeitpunkt das passende Personal mit dem notwendigen Wissen zu akquirieren. Zusätzlich ist es keine Selbstverständlichkeit, dass passende Linux-Schulungsangebote am Markt verfügbar sind, um bestehendes Personal weiterzubilden. Zugeschnittene Trainingsprogramme oder Zertifizierungspfade für Linux-Distributionen sind aktuell nur durch wenige Anbieter:innen verfügbar. Besteht die Anforderung an ein ganzheitliches Programm in deutscher Sprache, fallen weitere Anbieter:innen weg.

Anbieter:innen von Enterprise-Distributionen bieten neben reinen Schulungsangeboten vorbereitete Pfade zum Wissensaufbau z. B. SUSE Certified Administrator oder den Red Hat Certified Engineer an. Die Nutzung eines solchen Angebotes erleichtert dem Unternehmen die Personalentwicklung durch eine vordefinierte, aktuelle Wissensvermittlung für die jeweilige Rolle des Personals z. B. Supportmitarbeiter:in, Administrator:in oder IT-Architekt:in.

Neben der Erleichterung der gezielten Personalentwicklung spielen auch Zertifizierungsprogramme der Enterprise-Distributionen eine wichtige Rolle bei der externen Personalbeschaffung. Dies vereinfacht die Personalauswahl deutlich, da notwendiges Wissen bei Bewerber:innen bereits nachweislich belegt werden kann.

Auswahl der Linux-Distribution

Auswahl der Linux-Distribution

Die Grundlage für die **Entwicklung des Linux-Arbeitsplatzes** ist die Wahl der passenden GNU-/Linux-Distribution [im Folgenden kurz: Linux-Distribution]. Die Linux-Distribution stellt einen Betriebssystemkern und aufeinander abgestimmte Softwareanwendungen bereit.

Damit stellt die Distribution die Grundlage für die Softwareausstattung [Paketformat] und die kompatiblen Komponenten des Systemmanagements dar. Die Entscheidung für eine Linux-Distribution ist im Kontext des Linux-Arbeitsplatzes nicht ohne detaillierte Analyse möglich, da mit ihr weitere Dienstleistungen im Zusammenhang stehen und beachtet werden müssen. Dies macht ein Vergabeverfahren zur Entscheidungsfindung notwendig.

Vergaberechtlichte Aspekte

Dataport ist als Anstalt des öffentlichen Rechts öffentlicher Auftraggeber im Sinne des § 99 des Gesetzes gegen Wettbewerbsbeschränkungen [GWB]. Bei der Vergabe öffentlicher Aufträge hat Dataport daher die einschlägigen vergaberechtlichen Bestimmungen des GWB sowie weitere Vorgaben zu beachten. Diese hängen vom geschätzten Auftragswert ab. Zu den relevanten Vorgaben gehören die Verordnung über die Vergabe öffentlicher Aufträge [Vergabeverordnung, VgV], die Verfahrensordnung für die Vergabe öffentlicher Liefer- und Dienstleistungsaufträge unterhalb der EU-Schwellenwerte [Unterschwellenvergabeverordnung, UVgO] sowie weitere landesrechtliche Vorgaben des Landes Schleswig-Holstein. Der geschätzte Auftragswert ist auch maßgebliches Kriterium für die erforderliche Reichweite der Auftragsbekanntmachung [national oder EU-weit].

Bei einer Linux-Distribution handelt es sich um Open-Source-Software – dies wirft die Frage auf, warum wir uns mit einem Vergabeverfahren auseinandersetzen müssen? Viele Linux-Distributionen sind Sammlungen von meist freier und Open-Source-Software und können kostenfrei genutzt werden. Sofern der:die Auftraggeber:in keinen Vertrag über entgeltliche Liefer- oder Dienstleistungen i. S. d. § 103 GWB abschließt, unterliegt er:sie nicht dem Vergaberecht. Allerdings ist es im Enterprise-Umfeld zwingend notwendig, dass Supportdienstleistungen zur Verfügung stehen, damit Fehler zeitnah und nachhaltig behoben werden. Dies ist besonders im Bereich der öffentlichen Verwaltung relevant, damit bürgernahe Dienstleistungen zuverlässig und sicher erbracht werden können. **Eine Umstellung des Arbeitsplatzes auf das Linux-Betriebssystem bedeutet nicht nur die Ausstattung mit einer Linux-Distribution, sondern es muss zusätzlich für die Bereitstellung von Supportdienstleistungen gesorgt werden.** Sofern die entsprechende Expertise im Haus nicht vertreten ist, müssen entsprechende Leistungen von extern eingekauft werden.

Fortsetzung ▸

Wenn Software und weitere Leistungen wie Support, Wartung oder Entwicklung neuer Funktionen zeitnah beschafft werden, müssen diese zusammen betrachtet werden. Grundsätzlich muss der:die Auftraggeber:in seine Anforderungen in einer Leistungsbeschreibung formulieren, die allen Unternehmen den gleichen Zugang zum Vergabeverfahren ermöglicht [§ 31 VgV, § 23 UVgO].

Öffentliche Aufträge werden im Wettbewerb in transparenten und diskriminierungsfreien Verfahren vergeben [§ 97 GWB]. Ein Festlegen auf eine bestimmte Distribution ist vergaberechtlich nur unter bestimmten eingegrenzten Umständen zulässig. Dies ist beispielsweise der Fall, wenn die technischen Anforderungen nur durch ein bestimmtes Produkt erfüllt werden können.

Markt**erkundung**

In Vorbereitung des Vergabeverfahrens hat eine Markterkundung stattgefunden. Im Zuge dessen hat Dataport im Frühjahr 2021 im Auftrag des ZIT eine Analyse durchgeführt. Im Verfahren der Marktanalyse wurden bekannte und am weitesten verbreitete Linux-Distributionen betrachtet, um ihre Eigenschaften kennenzulernen und Konditionen für verschiedene Leistungen zu eruieren. Es wurden verschiedene Anbieter:innen angefragt, um eine realistische Einschätzung beispielsweise zu Angebotsumfang und Kosten zu erhalten. Die Einschätzung des Marktes unterstützt die Vorbereitung des Vergabeverfahrens.

Es gibt verschiedene Anbieter:innen von Linux-Distributionen. Wir unterscheiden dabei drei Distributionstypen entsprechend ihrer Entstehung, der Art ihrer Vermarktung und Supportmöglichkeiten:

- **Enterprise-Distribution:**
  Distribution, die von einem:einer kommerziellen Anbieter:in [Distributor:in] herausgegeben wird. Sie wird finanziert durch Support-Subskriptionsverträge und zielt auf Unternehmenskundschaft ab. Im Gegenzug erhält die Kundschaft je nach Umfang der Subskription z. B. technischen Support und einen Zugang zu Updates. Aufgrund der Eigenschaft von Open-Source-Software ist der Quellcode der Open-Source-Bestandteile der Distribution einsehbar. Einsichtnahme in Quellcode ist jedoch eher etwas für erfahrene Anwender:innen bzw. Entwickler:innen. Enterprise-Distributor:innen gewährleisten häufig eine lange Unterstützung und Stabilität der herausgegebenen Software.

- **Community-Distribution**
  Distribution, die von einer Gemeinschaft [Community] von Entwickler:innen veröffentlicht wird. Der Einsatz in Unternehmen ist prinzipiell möglich. Einen vertraglich zugesicherten Support kann die Community nicht leisten. Enterprise-Support ist für die großen Community-Distributionen über distributionsnahe IT-Dienstleister:innen verfügbar. Die Weiterentwicklung der Distribution findet in der Regel in der Community statt. Ein:eine IT-Dienstleister:in kann auf die Distribution nur in geringem Maße Einfluss nehmen.

- **Community-Enterprise-Distribution**
  Mischform aus den beiden vorherigen Ansätzen: Die Distribution wird von einem Softwareunternehmen entwickelt, ist jedoch frei verfügbar und für jeden Einsatzzweck nutzbar. Der Distributor betreibt Community-Management rund um sein Distributionsprodukt. Dadurch gibt es freiwillige Entwickler:innen, die an der Distribution mitwirken. Anwender:innen können alternativ zum Einsatz der freien Variante auch Enterprise-Support beim Distributor erwerben und damit den Einsatz der Distribution im eigenen Unternehmen absichern.

Vorbereitung des **Vergabeverfahrens**

Perspektivisch soll ein Großteil der Arbeitsplätze der Landesverwaltung in Schleswig-Holstein auf Linux umgestellt werden. Aus diesem Grund wird ein Vergabeverfahren vorbereitet, das den Betrieb und benötigte zusätzliche Leistungen ausschreiben wird. Wir legen uns nicht auf eine konkrete Distribution fest. Die Anbieter:innen der Distribution können sich von den Dienstleister:innen für weitere Leistungen unterscheiden. Insbesondere im Fall einer reinen **Community-Distribution** [s. „Markterkundung" S. 74] wird professionelle Leistung von Dritten nötig sein, da keine direkten Aufträge an die Community möglich sind.

Derzeit werden die Vergabeunterlagen ausformuliert und mögliche Kriterien aufgestellt, die aus Sicht Dataports und der Landesverwaltung Schleswig-Holstein in eine Bewertung einbezogen und daher in der Ausschreibung berücksichtigt werden müssen. Im Rahmen der Vergabe werden deshalb sowohl die Eigenschaften der Linux-Distribution selbst als auch die Eigenschaften der weiteren benötigten Leistungen spezifiziert werden. Diese Kriterien umfassen zusätzlich zu den technischen und funktionalen auch nicht funktionale Anforderungen. Gleichzeitig wird die Wichtigkeit der Kriterien bewertet. Die Anforderungen und Bewertungskriterien werden offengelegt werden. Die Entscheidung über die Distribution für den Linux-Arbeitsplatz wird zum Abschluss des Vergabeverfahrens durch Zuschlag auf das wirtschaftlichste Angebot unter Berücksichtigung des besten Preis-Leistungsverhältnisses erfolgen [gem. § 127 GWB].

Wichtige Bewertungskriterien werden der Beitrag zur digitalen Souveränität, aber auch die Integrierbarkeit in die technischen und personellen Prozesse von Dataport sein. Besonders hervorzuheben ist der bereits angesprochene Support im Enterprise-Umfeld. Aber auch Aspekte wie Planbarkeit, Verlässlichkeit und die Möglichkeit, technische Anforderungen einzubringen, werden eine Rolle spielen. Alle endgültigen Kriterien werden im Rahmen des Vergabeverfahrens im Detail veröffentlicht.

Indikation zur **Wirtschaftlichkeit**

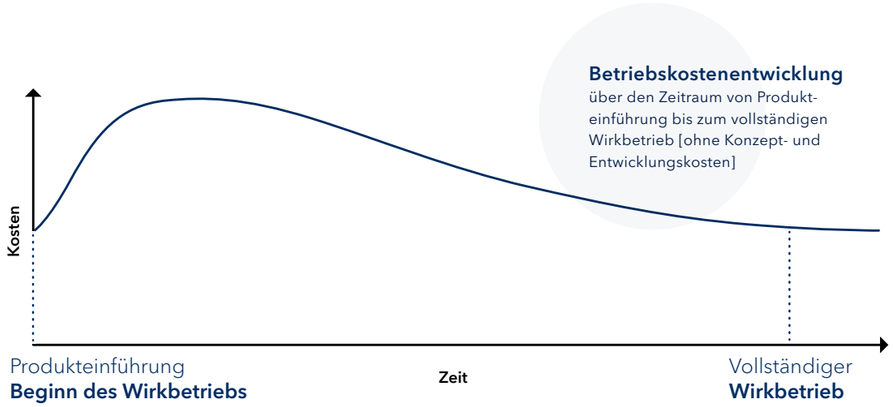
Indikation zur **Wirtschaftlichkeit**

In Anlehnung an das „Konzept zur Durchführung von Wirtschaftlichkeitsbetrachtungen [WiBe] in der Bundesverwaltung, insbesondere beim Einsatz der IT“ wurde im Rahmen der Machbarkeitsstudie zur neuen Linux-Arbeitsplatz-Modelllinie für die öffentliche Verwaltung in Schleswig-Holstein, durchgeführt im Jahr 2020, eine Indikation zur Wirtschaftlichkeit erstellt.

Der Detailgrad des Gesamtauftrages, inklusivesiver aller Entwicklungsleistungen, war zum damaligen Zeitpunkt nicht hoch genug, um belastbare Kosten oder Nutzen vollumfänglich zu definieren. Eine vollständige Wirtschaftlichkeitsbetrachtung nach dem Konzept WiBe 5.0 muss in einer zukünftigen Projektphase, in Bezug auf die hier entwickelte Indikation, durchgeführt werden.

Vorgehensweise

Die Entwicklungskosten eines Linux-Arbeitsplatzes für das Land Schleswig-Holstein teilen sich grundsätzlich in Planungskosten, Entwicklungs- und Investitionskosten sowie Kosten für die Systemeinführung [Migrationskosten] auf. Die Entwicklungskosten konnten zum Zeitpunkt der Machbarkeitsstudie 2020 nicht beziffert werden. Kosten für die Systemeinführung wurden im Rahmen der Indikation zum Zeitpunkt der Machbarkeitsstudie 2020 ebenfalls noch nicht berücksichtigt. Die hier vorgestellte Indikation berücksichtigt daher ausschließlich Betriebskosten und -nutzen für den Zeitraum von der Produkteinführung bis zum voraussichtlich vollständigen Wirkbetrieb [**vgl. Abbildung „Betriebskostenentwicklung“**].



Betriebskostenentwicklung
über den Zeitraum von Produkteinführung bis zum vollständigen Wirkbetrieb [ohne Konzept- und Entwicklungskosten]

Kostenmodell Betriebskosten und Betriebsnutzen

Betrachtet wird im Modell die neue IT-Maßnahme „Betrieb einer Linux-Modelllinie“. Mit Beginn der Umsetzung dieser neuen IT-Maßnahme fallen Betriebskosten und Betriebsnutzen an. Im Modell werden alle Kosten betrachtet, die aus dem Einsatz der neuen IT-Maßnahme entstehen. Der Betriebsnutzen entsteht als Einsparung, die sich aus dem Wegfall der Kosten der alten IT-Maßnahme ergeben.

Die Umsetzung der neuen IT-Maßnahme erfolgt ggf. unter sukzessiver Ablösung der alten IT-Maßnahme „Betrieb einer Windows-Modelllinie“. Für die Migrationsphase fallen entsprechend Kosten für beide IT-Maßnahmen an. Der Nutzen wird sukzessiv mit dem Ablösen der alten IT-Maßnahme gesteigert. Mit dem Übergang zum vollständigen Wirkbetrieb der neuen IT-Maßnahme wird ein konstantes Kosten-Nutzen-Verhältnis für die beim vollständigen Wirkbetrieb definierte Anwenderzahl angenommen. Im Rahmen der WiBe wird eine Preisindikation aus dem Verhältnis von Kosten [Kosten der neuen IT-Maßnahme] und Nutzen [Nutzen aus dem Wegfall der alten IT-Maßnahme] ermittelt und zusammenfassend in der nebenstehenden **Tabelle „Kostenmodell”** schematisch dargestellt. Die einzelnen Kriterien werden in den folgenden Abschnitten näher erläutert. Fortsetzung ▸

Kostenmodell
Betriebskosten und Betriebsnutzen

	Kriterium	Indikation
1	**Leitungs- und Kommunikationskosten**	≈
2	**Kosten für Infrastruktur und Dienste** WiBe 5.0: Host- und Serverkosten	≈
3	**Kosten für Arbeitsplatzrechner**	≈
4	**Softwarekosten**	▼
5	**Kosten externer Unterstützung**	▲
6	**Sonstige Kosten**	≈

Leitungs- und Kommunikationskosten

Das Kriterium „Leitungs-/Kommunikationskosten" umfasst alle Kosten [inklusive Netzkosten], die aufgrund der IT-Maßnahme von Leistungserbringer:innen bereitgestellt werden.

Diese Leistungserbringer:innen sind u. a.:

- **Kommunikationsdiensteanbieter:innen außerhalb der öffentlichen Verwaltung**
- **Behördenübergreifende Kommunikationsdiensteanbieter:innen innerhalb der öffentlichen Verwaltung**
- **Behördeninterne Kommunikationsdiensteanbieter:innen**

Die Umsetzung der IT-Maßnahme hat nur minimalen Einfluss auf die genannten Leitungs- und Kommunikationskosten. Die vorhandenen Dienste müssen voraussichtlich nicht zusätzlich erweitert werden. Während der Migration ist mit einer mengenmäßigen, aber nur kurzfristigen Zusatzbelastung der Dienste zu rechnen. Es wird angenommen, dass die Zusatzbelastung aufgrund des beschränkten Zeitraumes zu vernachlässigen ist und keine relevanten Kostensteigerungen zur Folge hat.

Infrastruktur und Dienste

WiBe 5.0: Host- und Serverkosten

Das Kriterium bezieht sich auf kalkulatorische Kosten, die durch die neue IT-Maßnahme im zentralen Rechenzentrum und im Serverbetrieb verursacht werden. Sofern die neue IT-Maßnahme Aufrüstungen erforderlich macht, sind diese haushaltswirksam. In diesem Kriterium sind auch Wartungs- und Pflegekosten sowie Ersatz-/Ergänzungskosten während des Wirkbetriebs zu berücksichtigen. Es sind ebenfalls Kosten für Datenschutz und Datensicherheit zu berücksichtigen.

Die Kosten für die zentrale Domain-Infrastruktur im Rechenzentrum bleiben nach aktuellem Kenntnisstand mittelfristig unverändert. Mit der Umsetzung der Maßnahme werden sich weiterhin Benutzer:innen- und Computerkonten über die bestehende zentrale Lösung authentifizieren. Ebenso bleiben die Kosten für die zentrale Überwachung sowie das Monitoring des Microsoft Active Directorys bestehen.

Spezifische Kosten für zentrale Dienste der alten IT-Maßnahme, wie zentrale „Windows Server Update Services" [WSUS] für das Update-Management von Microsoft-Betriebssystemen, können mit dem vollständigen Wirkbetrieb der neuen IT-Maßnahme reduziert oder eingespart werden.

Die Kosten für eine Installationsinfrastruktur bewegen sich aufgrund identischer Anforderungen im gleichen Rahmen wie bei der bestehenden IT-Maßnahme.

Kosten, die sich aus dem Vorhalten einer Infrastruktur zum Administrieren der Endgeräte ergeben, werden weiterhin Bestand haben. Linux-Distributionen lassen sich nicht durch den bestehenden zentralen AD-Verzeichnisdienst konfigurieren. Es ist mit zusätzlichen Kosten für den Betrieb von weiteren zentralen und ggf. dezentralen [für den Linux-Arbeitsplatz spezifischen] Managementkomponenten zu rechnen.

Mit einem längerfristigen Parallelbetrieb der alten und der neuen IT-Maßnahme ist zu rechnen.

Betriebliche Kosten bzgl. des Datenschutzes oder der Datensicherheit bleiben unverändert. Insgesamt wird keine signifikante Kostensteigerung im Bereich Infrastruktur und Dienste [Host- und Serverkosten] angenommen.

Kosten für Arbeitsplatzrechner

In diesem Kriterium werden Ersatz-/Ergänzungskosten während des Wirkbetriebs berücksichtigt. Beschaffungskosten, die vor Eintritt in den Wirkbetrieb entstehen, werden nicht hier, sondern bei den Entwicklungskosten, also außerhalb dieses Betriebsmodells erfasst.

Ggf. sind anfallende Wartungs- und Pflegekosten sowie Kosten für Datenschutz/ Datensicherheit zu berücksichtigen.

Mit der Umsetzung der neuen IT-Maßnahme kann voraussichtlich ein Großteil der bestehenden Hardware weiterhin genutzt werden. Dies gilt für Hardware und zugehörige Peripherie aus dem bestehenden Rahmenvertrag für Hardware-Beschaffung in Schleswig-Holstein [Stand 06/2021]. Spezialkonfigurationen werden in diesem Zusammenhang nicht betrachtet.

In der Machbarkeitsstudie 2020 wurden zwei repräsentative Notebooks aus dem seinerzeit aktuellen Kundenwarenkorb für Hardware mit gängigen Linux-Distributionen erfolgreich getestet.

Die Systemarchitektur von Linux-Betriebssystemen unterscheidet sich grundlegend von der Architektur aktuell genutzter Lösungen. Daher sind ggf. Anpassungen oder neue Prozesse für die Arbeitsplatzverwaltung zu entwickeln. Die hierdurch entstehenden Kosten sind Bestandteil der Entwicklungsphase. Weitere Kosten könnten sich durch den zusätzlichen Testaufwand im Rahmen des Hardwaremanagements ergeben.

Mit dem vollständigen Wirken der neuen IT-Maßnahme werden, neben den typischen Kosten für Reinvestitionen in neue Endgeräte-Hardware, keine signifikanten zusätzlichen Kosten bzgl. des Endgerätebetriebs angenommen.

Softwarekosten

In diesem Kriterium werden Kosten für zusätzliche Lizenzen, Lizenzerweiterungen, Wartung, Pflege und Updates während des Wirkbetriebs berücksichtigt. Beschaffungskosten, die vor Eintritt in den Wirkbetrieb entstehen, werden nicht an dieser Stelle, sondern bei den Entwicklungskosten erfasst.

Ggf. sind zusätzliche Kosten für Datenschutz und Datensicherheit sowie zur Barrierefreiheit zu berücksichtigen.

Es werden nur Softwarekosten betrachtet, die mit dem Betrieb der Endgeräte, dem Management der Endgeräte sowie der Bereitstellung von Diensten im Rahmen des Arbeitsplatzes im direkten Zusammenhang stehen.

Eine vollumfängliche Aussage bzgl. zusätzlicher Lizenzkosten für Produkte der neuen IT-Maßnahme kann zu diesem frühen Zeitpunkt nicht getätigt werden. Für den Einsatz der neuen IT-Maßnahme kommen sowohl Produkte infrage, die einmalige oder laufende Lizenzkosten verursachen, als auch lizenzkostenfreie. Eine realistische Aussage bzgl. zusätzlicher Lizenzkosten kann erst in folgenden Projektphasen erfolgen.

Fortsetzung ▸

Eine Kostenreduzierung durch Ablösung der alten IT-Maßnahme, bzgl. der Lizenzkosten für den Endgerätebetrieb, ist anzunehmen. Der Umfang der bestehenden Lizenzverträge mit Microsoft kann sukzessive reduziert werden. Sofern weiterhin Infrastrukturkomponenten des Herstellers Microsoft eingesetzt werden, sind hierfür weiterhin Zugriffslizenzen [Client Access License – CALs] erforderlich.

Zu diesem Zeitpunkt der Konzeption gehen wir insgesamt von einer Kostenreduzierung aus. Synergieeffekte können durch einen vorab erfolgten oder parallelen Umstieg auf eine lizenzkostenfreie Office-Softwarelösung auf den Arbeitsplätzen der Landesverwaltung in Schleswig-Holstein erzielt werden.

Kosten externer Unterstützung

Soweit während des Wirkbetriebs Kosten für externe Unterstützung anfallen, werden diese hier berücksichtigt. Kosten für externe Beratung und Unterstützung, die vor Eintritt in den Wirkbetrieb entstehen, werden bei den Entwicklungskosten erfasst.

Es werden voraussichtlich Kosten für externe Unterstützung im Wirkbetrieb der neuen IT-Maßnahme anfallen. Ein Kostenfaktor könnte der Einkauf von Enterprise-Support für die auf dem Arbeitsplatz eingesetzte Linux-Distribution oder damit verbundene Managementdienste sein. Eine weitere Kostenquelle könnte sich aus dem Einkauf von Fremdpersonal für die Weiterentwicklung des Arbeitsplatzes oder des Systemmanagements sowie auch für die Implementierung von Schnittstellen zu Fachverfahren ergeben. Der Einkauf von externem Fremdpersonal erzeugt meist deutlich höhere Kosten als der Einsatz von Dataport-eigenem Personal.

Sachkosten für den Einkauf von Personalschulungen werden unvermeidbar anfallen. Ein Teil dieser Sachkosten wird bereits in der Entwicklungsphase anfallen. Weitere Kosten während des Wirkbetriebs für externes Personal, im Rahmen von Schulungen, sind anzunehmen, da die Migration auf die neue IT-Maßnahme während des Wirkbetriebs stattfindet. Es müssen die Schulungskosten für IT-Fachpersonal als auch für Anwender:innen bedacht werden.

Eine weitere Kostenquelle wird sich aus dem Einkauf von externem Personal im Rahmen der Arbeitsplatzsupportprozesse [Anwender.innensupport 1st Level] ergeben.

Sonstige Kosten

Unter diesem Kriterium werden die Kosten veranschlagt, welche von den vorangehenden Kriterien nicht abgedeckt sind [z. B. Entsorgungskosten].

Entsorgungskosten werden durch aktuelle Verträge abgedeckt und diese müssen auf die neue IT-Maßnahme abgestimmt werden. Kosten für neue Konzepte werden im Rahmen der Entwicklungsphase veranschlagt. Die Entsorgungskosten im Wirkbetrieb werden voraussichtlich identisch zu denen der bestehenden IT-Maßnahme sein. ●

© Unsplash.com / Krakenimages

Risiken

9

Risiken

Die nachfolgenden Abschnitte beschreiben verschiedene Blickwinkel einer **Risikoeinschätzung für die Einführung einer neuen Arbeitsplatz-Modelllinie auf Basis von GNU / Linux**. Diese Risiken umfassen neben wirtschaftlichen Risiken auch technische, organisatorische und politische Risiken. Die folgenden Aufzählungen erheben keinen Anspruch auf Vollständigkeit über alle Detailebenen.

Einstufung der Risiken

Risiken lassen sich zur Bewertung kategorisieren. Eine bekannte Methode ist die sogenannte ALARP-Matrix[23] [vgl. Abbildung S. 87], welche Risiken gemäß ihrer **Eintrittswahrscheinlichkeit [E]** und ihres **Schadensausmaßes [S]** einteilt. Risiken im grünen Bereich werden in der Regel als vertretbar angesehen.

[23] **ALARP**
[engl. „as low as reasonably practicable" = „so niedrig wie vernünftigerweise praktikabel"] meint ein Prinzip der Risikoreduzierung. Dies besagt, dass Risiken so weit reduziert werden sollen, dass es auch noch praktisch vertretbar ist.

Wirtschaftliche Risiken

„Das Ziel einer wirtschaftlichen Steuerung von IT-Risiken ist es, die zuvor identifizierten und quantifizierten [Risiken] unter Kosten-/Nutzen-Aspekten gezielt zu beeinflussen und zu reduzieren. Da IT-Risiken Verluste darstellen, wirkt sich dies[e Beeinflussung] positiv auf das Unternehmensergebnis aus."[24] Anders als in den meisten Wirtschaftsunternehmen ist es den Behörden möglich, Investitionsprojekte mit „längerem Atem" zu tätigen, in Bereichen für die ein nicht geringes Risiko anzunehmen ist [Pionierarbeit]. Bei der Umstellung auf Open-Source-basierte IT-Systeme spielt insbesondere das zu erzielende, nicht direkt ökonomisch abschätzbare Endergebnis der „digitalen Souveränität" eine essenzielle Rolle. Nichtsdestotrotz ist es deshalb gerade deshalb erforderlich, auf diesem noch unsicheren Terrain Risiken gut vorherzusagen und Absicherungsmaßnahmen zu treffen.

[24] **Wirtschaftliche Steuerung von IT-Risiken**
Vgl. Prokein, 2008

Kostenverschiebungen

Open-Source wird in der öffentlichen Wahrnehmung oft mit „gratis" gleichgesetzt. Die finanzielle Komplexität und der Aufwand einer Migration werden gern unterschätzt.

Zum einen werden Einsparungen bei den Lizenzkosten falsch eingeschätzt, die nur einen Teil der IT-Kosten ausmachen. Die Supportkosten einer individuellen, eigenen Lösung [z.B. eine stark angepasste Linux-Distribution] sind [teilweise] höher als bei der Verwendung einer vollständig proprietären Lösung [z.B. Produkte wie Enterprise-Linux-Distribution oder lizenzpflichtige Life-Cycle-Managementsoftware], bei der die Kosten für Support und die Weiterentwicklung durch einen:eine Hersteller:in kommerzieller Software [bzw. Enterprise-Distributor:in] von vornherein im Lizenzpreis einkalkuliert sind.

Insgesamt ist mit einer Einsparung an Lizenzkosten für die Linux-Arbeitsplatz-Modelllinie zu rechnen. Diese Einsparung wird voraussichtlich kostenmäßig in Richtung Support verschoben werden. Problematisch ist das Fehlen vorhandener Erfahrungswerte bei Dataport, sodass das exakte Ausmaß dieser Verschiebung noch nicht ausreichend abgeschätzt werden kann. Eine Absicherung vor diesem Risiko wird durch Aufbau eigener und Einkauf externer Linux-Expertise erfolgen.

Risikobewertung
„Kostenverschiebungen":
E = gelegentlich
S = geringfügig

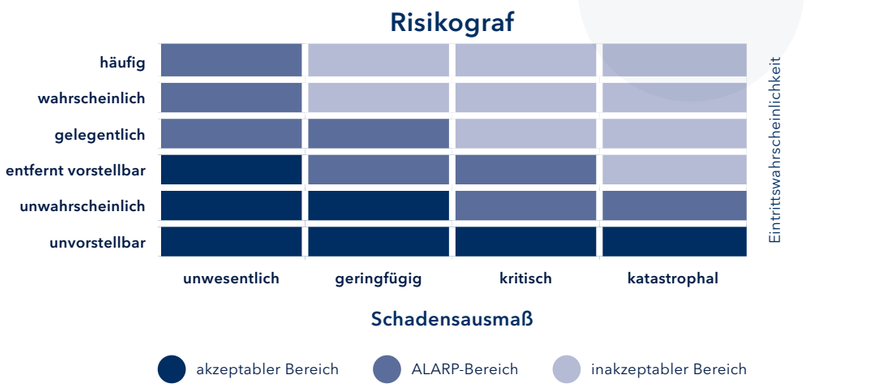
Betriebskosten für eigene Softwareanpassungen

Eine Stärke von Open-Source-Software, die mögliche Anpassbarkeit an spezifische Bedürfnisse [z.B. die einer öffentlichen Einrichtung], kann gegenüber einer proprietär-kommerziellen Lösung zu einem finanziellen Risiko werden. Die Pflege und die Weiterentwicklung von eigenen, individualisierten Softwarelösungen verursachen möglicherweise höhere Kosten [Gefahr des „ungewollten" Erstellens eines „Forks" einer OSS]. Beim sonst üblichen Entwicklungsmodell für proprietär-kommerzielle Software wird dieser Aufwand von dem:der Hersteller:in übernommen, welcher:welche die Kosten auf mehrere Kund:innen [teils weltweit] umlegen und damit kostengünstig sein kann. Deshalb können die Betriebskosten einer angepassten OSS-Lösung höher sein.

Eine mögliche Absicherungsmaßnahme kann sein, verwaltungsspezifische Entwicklungsprojekte Bundesländer-übergreifend zu finanzieren und/oder zu realisieren. Bei Anpassung von bereits existierender OSS mit breiterer Anwender:innenbasis stellt eine enge Kooperation mit den Up-stream-Projekten dieser Software eine mögliche Absicherungsmaßnahme dar. Grundsätzlich ist die Entwicklung vieler einzelner, individueller Lösungen [und dem daraus erfolgenden Wartungsaufwand dieser Lösungen] zu vermeiden.

Risikobewertung
„Betriebskosten für eigene Softwareanpassungen":
E = gelegentlich
S = geringfügig

ALARP-Matrix
https://de.wikipedia.org/wiki/ALARP



LINUX-STUDIE **RISIKEN**

Technische Risiken

Das technische Risikomanagement erfasst den gesamten Life-Cycle eines Linux-Arbeitsplatzes sowie den Betrieb der Modelllinie und ihrer Infrastruktur insgesamt. Eine zukünftige Ergänzung der unten angeführten Aufzählung ist wahrscheinlich. Es sollen langfristig alle Produktphasen der Modelllinie miteinbezogen werden [von der Konzeptionierung bis zur Entsorgung].

Komplexität

Die Einführung einer Linux-Arbeitsplatz-Modelllinie bringt eine Vielzahl von Prozess- und Infrastrukturanpassungen auf technischer Ebene mit sich. Das komplexe System an Abhängigkeiten kann unvollständig erfasst werden [aus Mangel an Fachexpertise für gemischte Windows-Linux-Infrastrukturen], was Nachsteuerungen und Verzögerungen im Projektverlauf nach sich ziehen kann.

Der Migrationsaufwand [Zeit, Infrastrukturanpassungen etc.] einzelner Abhängigkeiten kann falsch eingeschätzt werden: Z.B. sind die wenigsten Softwareprodukte einfach komplett austauschbar. Es kann zu zeitaufwendigen Kleinstmigrationen kommen [z.B. Microsoft-Office-Makros gegen Open-Office-Makros ersetzen].

Eine Absicherung kann durch eine weitsichtige Projektsteuerung und ausreichend frühzeitig begonnene vorbereitende Maßnahmen [**vgl. S. 61**] erfolgen.

Risikobewertung
„Komplexität“:
E = wahrscheinlich
S = kritisch

Fachanwendungen

Bzgl. der im Land Schleswig-Holstein genutzten Fachverfahren müssen verschiedene Maßnahmen für die Gewährleistung von Kompatibilität im Vorfeld geleistet werden.

Sämtliche Fachanwendungen müssen beim Umstieg der Anwender:innen auf ein Linux-basiertes Endgerät voraussichtlich an betriebliche Prozesse angepasst werden. Auch bei Verfügbarkeit alternativer, funktional äquivalenter Open-Source-Produkte ist ein ggf. komplexer und aufwendiger Migrationsprozess notwendig. Der Aufwand dieser Anpassungsmaßnahmen kann unterschätzt werden.

Viele Fachanwendungen werden nicht von Dataport bereitgestellt, sondern von IT-Abteilungen in den Landesbehörden. D.h., viele der Fachverfahren sind dem IT-Dienstleister Dataport [noch] gar nicht explizit bekannt. Beim Einkauf neuer Fachverfahren gab es bislang wenige Vorgaben bzgl. der technischen Eigenschaften eines zu beschaffenden Softwareprodukts. Eine Fehleinschätzung des notwendigen Aufwands ist denkbar. **Hier sind zukünftig klarere Vorgaben für Neuanschaffungen notwendig sowie kurz- bis mittelfristig eine Erfassung der bereits beschafften und genutzten Fachanwendungsprodukte.** [25]

Eine Fehleinschätzung der Abhängigkeiten zwischen Fachanwendungsportierungen und Einführung der Linux-Arbeitsplatz-Modelllinie kann zu globalen Projektverzögerungen führen. Ein Unterschätzen des Aufwands für die einzelnen Fachanwendungsportierungen kann zu Roll-Out-Verzögerungen in einzelnen Behördenabschnitten führen.

Als Grundvoraussetzung für eine gute Rollout-Planung wird aktuell ein Projekt zur Katalogisierung der Fachanwendungslandschaft in den Landesbehörden von Schleswig-Holstein vorbereitet.

Fachwendungen mit breiter Nutzer:innenbasis im Land SH sollten frühzeitig plattformunabhängig neuentwickelt oder ggf. auf Linux portiert werden [parallel zur Entwicklung der neuen Modelllinie]. Alternative Bereitstellungsmethoden [z.B. vorübergehend als Terminalservices] können aus strategischer Sicht nur kurzfristige Lösungen sein. Für spezifische Fachanwendungen einzelner Behörden ist jedoch nicht mit einer zeitnahen Linux-Portierung zu rechnen. Diese sollten daher deutlich vor Rollout-Termin der Linux-Arbeitsplätze im jeweiligen Behördenabschnitt auf eine alternative Bereitstellungsplattform migriert werden. Diese migrierten Fachanwendungen wären dann von der alten und der neuen Modelllinie aus nutzbar. Die Nutzung der migrierten Fachanwendungen könnte direkt nach Migration der Anwendung einsetzen, auch wenn der Arbeitsplatz noch nicht auf Linux umgestellt wurde [Konsolidierung der neuen Bereitstellungsmethode].

Langfristig ist eine Vereinheitlichung der Bereitstellung aller Fachverfahren in Form von Webservices erforderlich. Wichtigste Anforderung hierfür ist: plattformübergreifende Nutzbarkeit des Fachverfahrens [d.h. unabhängig von der Architektur des Endgeräts, auch touchbasierte Bedienung sollte unterstützt sein]. Durch eine solche Standardisierung müsste nicht jede einzelne Fachanwendung für eine zusätzliche Endgerätearchitektur portiert werden. Es müsste lediglich die Kompatibilität zwischen Webbrowser des Endgeräts und der jeweiligen Fachanwendung geprüft werden.

Eine Vereinheitlichung bei der Bereitstellung von Fachverfahren ist losgelöst von der Einführung einer neuen Arbeitsplatz-Modelllinie basierend auf dem Linux-Betriebssystem. Für Fachanwendungen mit einer breiten Nutzer:innenbasis ist es generell sinnvoll, die Software langfristig auch auf anderen Devices [andere Betriebssysteme, andere Endgerätetypen] und für andere Bedienkonzepte [insbesondere touchbasierte Eingaben am Tablet] nutzbar zu machen. Sehr spezielle Fachverfahren hingegen, die für einen sehr spezifischen Anwendungskontext entwickelt worden sind, müssen wahrscheinlich noch sehr langfristig ohne Anpassung weiter betrieben und genutzt werden [können].

Eine weitere Konsolidierung kann über Absprache der verschiedenen Ressorts bzgl. der genutzten Softwareprodukte erfolgen. Es sind Fälle bekannt, wo [zu] viele verschiedene Softwareprodukte für den gleichen Einsatzzweck betrieben werden.

Risikobewertung
„Fachanwendungen“:
E = wahrscheinlich
S = kritisch

[25] **Vorgaben für Neuanschaffungen**
Hierzu wurde 2021 ein Analyseprojekt vom Land Schleswig-Holstein bei Dataport beauftragt, mit der Zielvorgabe, eine Vorgehensweise zu erarbeiten, um die im Land verwendeten Fachverfahren über alle Behörden und Ressorts hinweg zu katalogisieren.

Organisatorische Risiken

Zu den allgemeinen organisatorischen Risiken zählen z. B.:

- Die Akquirierung von genügend qualifiziertem Personal sowie dessen langfristige Bindung an den IT-Dienstleister Dataport
- Die Abstimmung von Qualifikationen des Personals auf die zugewiesenen Aufgabenstellungen
- Die [Un-]Vermeidbarkeit von Abhängigkeiten von externen Dienstleister:innen, Softwareherstellen:innen und den versch. Open-Source-Projekten
- Die Herausforderung bzgl. des Wissensmanagements [insbesondere bei Kooperation mit externen Dienstleister:innen]
- Das Zusammenspiel zwischen IT-Dienstleister:innen und der Gruppe der Anwender:innen

Organisatorische Risiken, die spezifisch für die Einführung einer auf Open Source basierenden Arbeitsplatz-Produktlinie eingeschätzt werden, werden im Folgenden näher betrachtet. [Es wird kein Anspruch auf Vollständigkeit erhoben.]

Open-Source-Communitys

Die Zusammenarbeit mit der Open-Source-Community wird bei Dataport noch nicht lange erprobt. Als allgemeine Beobachtung der OSS-Community wird eine starke Fragmentierung der sich um Linux versammelnden Teil-Communitys wahrgenommen. Die verschiedenen Strukturen von Open-Source-Projekten weisen einen hohen Grad an Diversität auf und viele Projekte werden nicht von Wirtschaftsunternehmen [mögliche Geschäftspartner:innen] unterstützt. Es gilt, für Community-Interaktionen projekt- bzw. produktspezifisch individuelle Vorgehensweisen bzgl. einer möglichen Zusammenarbeit zu entwickeln und diese langfristig zu vereinheitlichen. Vorgaben des Beschaffungsrechts sind hier unbedingt zu berücksichtigen.

Eine Maßnahme, um dieser Diversität von Projekten zu begegnen, ist der Aufbau der Position eines Open-Source-Community-Managements eigens für die Linux-Arbeitsplatz-Modelllinie. Das OSS-Community-Management wird über den Entwicklungszeitraum die technischen und organisatorischen Arbeiten im Hause Dataport begleiten und eine Schnittstelle zu den verschiedenen, involvierten OSS-Dienstleister:innen und -Communitys darstellen.

Risikobewertung
„Open-Source-Communitys“:
E = wahrscheinlich
S = geringfügig

Entwicklungszyklen von Linux-Distributionen

Die auf dem Linux-Arbeitsplatz zu verwendende Distribution wird das Ergebnis eines Vergabeverfahrens für Enterprise-Support sein. Unter Umständen wird dadurch eine Linux-Distribution zum Einsatz kommen, die Dataport wenig eigene Flexibilität bei der Gestaltung der Produktzyklen einräumen wird. Als Absicherung ist hier bei der Erstellung des Vergabeverfahrens darauf zu achten, dass die Anforderungen der eigenen Produkt- und Releasezyklen bereits erarbeitet sind und entsprechend in den Leistungsanforderungen beschrieben werden.

Ferner kann es vorkommen, dass [proprietäre] Standardsoftware [z. B. Zoom-Client, Skype etc.] nicht über die via Vergabeverfahren festgelegte Distribution bezogen werden kann. Hier gilt es, als Absicherungsmaßnahme Verfahren zu entwickeln, mit denen einzelne Softwarekomponenten des Linux-Arbeitsplatzes vom Releasezyklus der Distribution entkoppelt installiert und aktualisiert werden können [z. B. Bereitstellung in Container-Paketformaten o. Ä.].

Risikobewertung
„Entwicklungszyklen von Linux-Distributionen“:
E = gelegentlich
S = geringfügig

Akzeptanz der Anwender:innen

Migrationen von kommerzieller zu Open-Source-Software können aus mehreren Gründen stärker von schlechter Akzeptanz der Anwender:innen begleitet werden, als dies von Migrationen von und zu kommerziellen Softwareprodukten bekannt ist: Einerseits haben OSS-Produkte in der Öffentlichkeit manchmal ein Image-Problem. Man nimmt an, „kostenlose“ Produkte könnten per se nicht mit kommerziellen Lösungen konkurrieren. Die fehlende Öffentlichkeitspräsenz von OSS-Produkten, u. a. aufgrund geringerer Marketing-Budgets, führt zu der Wahrnehmung, sie sei weniger ausgereift als kommerzielle Software. Gepaart mit einer prinzipiell kritischen Haltung der Anwender:innen gegenüber Änderungen, kann dies zu einer starken Ablehnung gegenüber OSS-Lösungen führen.

Die Anwender:innen des Linux-Arbeitsplatzes in den Behörden müssen bei der Einführung der Linux-Arbeitsplatz-Modelllinie [bzw. bzgl. des Wegfalls der Microsoft-Office-Produktlinie] gezielt „mitgenommen“ werden. Die Migration der Dokumentenlage wird aufseiten der Verwaltungsmitarbeiter:innen einen hohen Aufwand an Umformatierungs- und Konvertierungsschritten mit sich bringen. Der allgemeine Nutzen dieses Arbeitsaufwandes [wie z. B. allgemein die „digitale Souveränität“ an sich, aber auch technische Aspekte wie z. B. bessere Barrierefreiheit in den Dokumenten] muss den Mitarbeiter:innen gut vermittelt werden. Es wird an dieser Stelle viel Gewinnungsarbeit zu leisten sein, um das Risiko einer Ablehnung der Linux-Arbeitsplatz-Modelllinie in den Verwaltungen zu reduzieren.

Risikobewertung
„Akzeptanz der Anwender:innen“:
E = gelegentlich
S = geringfügig

Politische Risiken

Die Umstellung auf eine Linux-Arbeitsplatz-Modelllinie in der Verwaltungslandschaft von Schleswig-Holstein ist ein auf hohe Langfristigkeit ausgelegtes Projekt. Demgegenüber steht ein fester fünfjähriger Wahlturnus aufseiten des Landesparlaments. Die Wirtschaftlichkeit einer auf Langfristigkeit ausgelegten Open-Source-Umstellung wird erst über mehrere Legislaturperioden hinweg sichtbar werden.

Neben langfristig wirtschaftlichen Einsparungen bietet die Umstellung auf Open-Source-Verfahren in der gesamten Landes-IT insbesondere auch einen ideellen Mehrwert. Das Zur-Kenntnisnehmen dieses Mehrwerts und dessen Förderungswürdigkeit muss in der politischen Strategie des Landes verankert sein und bleiben.

Abkehr von **Open-Source-Strategie**

In zukünftigen Legislaturperioden des Schleswig-Holsteinischen Landtags kann es zu veränderten politischen Formationen [Koalitionen] kommen, für die Open Source einen niedrigeren Stellenwert hat.

Ein Projekt wie von der Tragweite einer Betriebssystemumstellung auf den Verwaltungsarbeitsplätzen bedarf einer enormen strategischen Stabilität, welche sich innerhalb einer Behörde aus einer politischen Stabilität bzgl. der IT-Strategie auf der Ebene der Entscheider:innen ergibt. Ein Abwenden von der Open-Source-Strategie auf landespolitischer Ebene muss finanziell mit jeder Projektphase eigens bewertet werden.

Sicherlich wird ein frühzeitiges Abwenden von der aktuellen Open-Source-Strategie des Landes Investitionsverluste nach sich ziehen. Eine mögliche partielle Absicherungsmaßnahme gegen diese finanziellen Verluste könnte z.B. sein, die Neuausgestaltung der Dienstinfrastruktur für den Linux-Arbeitsplatz möglichst betriebssystemunabhängig zu konzipieren [und schon andere Arbeitsplatz-Plattformen vorzusehen]. Die neue Dienstelandschaft sollte somit in der Lage sein, verschiedenste [proprietäre und quelloffene] Betriebssysteme zu integrieren. Sollte eine übernächste Modelllinie nicht mehr auf dem Linux-Betriebssystem basieren, dann steht im Idealfall die Infrastruktur für diese übernächste Arbeitsplatz-Modelllinie schon bereit. Die Entwicklung einer nur auf Linux-Arbeitsplätze ausgerichteten Infrastruktur im Rahmen dieses Projekts wäre somit zu vermeiden.

Als weitere Absicherungsmaßnahme sollte zudem auch lange nach Inbetriebnahme von Open-Source-Infrastrukturen fortwährend auf politischer Ebene Open Source als IT-Strategie der Zukunft beworben werden. Die gute Informationsarbeit und transparente Berichterstattung zu einzelnen Projektfortschritten in Richtung Politik sollte auch Jahre nach einer Umstellung auf Open Source fortgesetzt werden. Die sich zu jeder Legislaturperiode teilweise wandelnde Gruppe der Landtagsabgeordneten muss kontinuierlich über die Stärken der Open-Source-Strategie des Landes unterrichtet werden. An dieser Stelle wird fortwährend Gewinnungsarbeit zu leisten sein.

Risikobewertung

„Abkehr von Open-Source-Strategie“:

E = entfernt vorstellbar
S = katastrophal

© pexels.com / Fauxels

Fazit & **Ausblick**

10

Fazit & Ausblick

Das Linux-Betriebssystem ist auf dem Arbeitsplatz **im wissenschaftlichen Umfeld und bei IT-Expert:innen weitverbreitet**. Der Gedanke, dieses Betriebssystem auch für eine breite Masse an Verwaltungsarbeitsplätzen zu nutzen, ist nachvollziehbar.

LINUX-STUDIE **FAZIT & AUSBLICK**

Die Qualität des Linux-Desktops hat im letzten Jahrzehnt deutlich zugenommen. Auch ein für Enterprise-Umgebungen notwendiges modulares Systemdesign lässt sich umsetzen. Intuitiv bedienbare Arbeitsoberflächen sind vorhanden und es existieren plattformübergreifende Open-Source-Anwendungen [z. B. LibreOffice, Firefox, Chromium], die den meisten Anwender:innen bereits vertraut sind. Weitere Anwendungen, z. B. Fachverfahren, lassen sich meist ohne Medienbruch in die Arbeitsoberfläche integrieren.

Dennoch ist ein Linux-Arbeitsplatz nur eine mögliche Antwort auf ein solches Endgeräte-Design. Das Ausrollen eines Linux-Betriebssystems auf den Arbeitsplätzen der öffentlichen Verwaltung ist kein Muss für mehr digitale Souveränität in der Verwaltungslandschaft. Vielmehr ist ein Verwaltungsarbeitsplatz unter Linux ein deutliches Signal nach außen sowie eine vollständige und medienwirksame Bekennung zu Open-Source. Und zugleich punktet ein Arbeitsplatz unter Linux deutlich besser in den Bereichen IT-Sicherheit [Auditierbarkeit durch Quelloffenheit] und Transparenz [Entwicklung des Arbeitsplatzes als Open-Source-Projekt].

In dieser Studie wurde die Vision eines Open-Source-Verwaltungsarbeitsplatzes mit den Anforderungen an den Betrieb eines solchen Arbeitsplatzes innerhalb einer Enterprise-Infrastruktur in Verbindung gesetzt. Im Ergebnis lässt sich der Wunsch nach mehr digitaler Souveränität sehr wohl mit den Anforderungen an einen modernen Arbeitsplatz innerhalb von mandant:innenfähigen Enterprise-Architekturen vereinbaren. Eine Umsetzung in der Praxis ist eindeutig machbar und der Betrieb von Linux-Arbeitsplätzen langfristig ähnlich wirtschaftlich wie die bisherige Microsoft-Windows-basierte Infrastruktur.

Durch aktuelle Virtualisierungstechnologien ist die betriebssystemunabhängige Bereitstellung einer heterogenen Anwendungslandschaft für Fachverfahren bereits heute weitgehend möglich. Langfristig muss die Fachverfahrenslandschaft in Schleswig-Holstein allerdings einen Wandel durchlaufen: Neue Fachanwendungen müssen zukünftig als plattformunabhängige Softwareentwicklungen beauftragt werden [d. h. als Webanwendung]. Das Ziel muss sein, Fachverfahren unabhängig vom Betriebssystem des Endgeräts nutzen zu können.

Im Zuge einer Machbarkeitsstudie im Jahr 2020 zeichnete sich ab, dass bei der Weiterentwicklung der Infrastruktur für zentrale Dienste ebenfalls Plattformunabhängigkeit in Bezug auf das Endgerät eine wichtige Rolle spielen muss. Die Infrastruktur muss zukünftig in der Lage sein, für unterschiedliche Betriebssystemplattformen und Softwarearchitekturen [Arbeitsplätze, Webanwendungen, Windows-Terminalserver-gestützte Anwendungen usw.] ihre Dienste, wie z. B. Anmeldedienst, Dateiablage, Druckdienst, über standardisierte und generische Schnittstellen bereitzustellen.

> DER WUNSCH NACH MEHR DIGITALER SOUVERÄNITÄT LÄSST SICH MIT DEN ANFORDERUNGEN AN EINE MODERNE IT-INFRASTRUKTUR VEREINBAREN.

Wirtschaftlich betrachtet ist die Einführung einer Linux-Arbeitsplatz-Modelllinie auf hohe Langfristigkeit ausgelegt. Einsparungen sind erst nach mehreren Jahren zu erwarten. In einer ersten Risikoabschätzung bzgl. der Einführung von Linux-Arbeitsplätzen in der Landesverwaltung Schleswig-Holstein wurden verschiedene Risiken herausgearbeitet und eine im Projektverlauf möglichst frühe Etablierung verschiedener Absicherungsmaßnahmen empfohlen.

Der Einsatz eines modernen Linux-Arbeitsplatzes wird für die Landesverwaltung Schleswig-Holstein ein deutlicher Schritt in Richtung von mehr digitaler Souveränität sein. Es soll als Leuchtturmprojekt weit über Schleswig-Holstein hinauswirken und wird langfristig einen gesellschaftlichen Mehrwert bieten. ●

Das Endgerät und die dafür betriebene Infrastruktur sind eng miteinander verzahnt. Beide in gleicher Weise zu betrachten spielt eine entscheidende Rolle.

Literatur

CDU, GRÜNE, FDP, 2017

Christlich Demokratische Union Deutschlands Landesverband Schleswig-Holstein, Bündnis 90/Die Grünen Landesverband Schleswig-Holstein, Freie Demokratische Partei Landesverband Schleswig-Holstein: Koalitionsvertrag für die 19. Wahlperiode des Schleswig-Holsteinischen Landtages [2017–2022] zwischen CDU, Bündnis 90/Die Grünen, FDP, S. 108.

Verfügbar unter ▸ https://www.schleswig-holstein.de/DE/Landesregierung/_documents/koalitionsvertrag2017_2022.pdf?__blob=publicationFile&v=1

PROKEIN, 2008

Oliver Prokein: IT-Risikomanagement, Kapitel 4 „Wirtschaftliche Steuerung von IT-Risiken", Gabler, 2008.

Verfügbar unter ▸ https://doi.org/10.1007/978-3-8349-9688-6_4

SCHLESWIG-HOLSTEINISCHER LANDTAG, 2018

Schleswig-Holsteinischer Landtag: Nutzung von Open-Source-Software, 2018.

Verfügbar unter ▸ http://www.landtag.ltsh.de/infothek/wahl19/drucks/00700/drucksache-19-00756.pdf

SCHLESWIG-HOLSTEIN LANDESREGIERUNG, 2020

Landesregierung Schleswig-Holstein: Bericht der Landesregierung „Nutzung von Open-Source-Software", 2020.

Verfügbar unter ▸ https://www.landtag.ltsh.de/infothek/wahl19/drucks/02000/drucksache-19-02056.pdf

Impressum

Herausgeber
Der Ministerpräsident des Landes Schleswig-Holstein
Düsternbrooker Weg 104 | 24105 Kiel

Kontakt
Zentrales IT-Management
CIO Chief Information Officer | Sven Thomsen
digitalisierung@melund.landsh.de

Entwickelt & gestaltet
in Zusammenarbeit mit Dataport AöR

Autor:innen
Sascha Kern, Nils Voss, Christian Kempe, Marita Blank-Babazadeh, Axel Hinz [Dataport];
Mike Gabriel [Fre(i)e Software GmbH]

Stand
April 2022

Web
www.schleswig-holstein.de/linux-arbeitsplatz

Abkürzungen

AD	**Verzeichnisdienst-Implementierung** [Engl. Active Directory]
ALARP	**Prinzip der Risikoreduzierung:** „so niedrig wie vernünftigerweise praktikabel" [Engl. für „as low as reasonably practicable"]
AöR	**Anstalt öffentlichen Rechts**
BSI	**Bundesamt für Sicherheit in der Informationstechnik**
CUPS	**Standard-Open-Source-Produkt im Unix-Bereich zur Ansteuerung von Druckerendgeräten** [Engl. für „Common Unix Printing System"]
ESM	**Sicherheitsmanagement in Unternehmen** [Engl. für „Enterprise Security Management"]
GNU	**Unix-ähnliches Betriebssystem ohne eigenen Betriebssystemkern** [Engl. für das rekursive Akronym „GNU's Not Unix"]
GUI	**Grafische Bedienoberfläche** [Engl. „Graphical User Interface"]
GWB	**Gesetz gegen Wettbewerbsbeschränkungen**
IAM	**Identitäts- und Zugriffsberechtigungsmanagement** [Engl. für „Identity and Access Management"]
INV+LOG	**Berichtswesen** [Engl. für „inventory" und „logging"]
KM	**Konfigurationsmanagement**
LCM	**Life-Cycle-Management**
LDAP	**Protokollstandard für die Kommunikation mit einem hierarchisch organisierten Verzeichnisdienst** [Engl. für „Lightweight Directory Access Protocol"]
MS	**Microsoft**
OSD	**Betriebssysteminstallation** [Engl. für „Operating System Deployment"]
OSS	**Open-Source-Software**
PM	**Patch-Management**
POSIX	**Betriebssystemspezifikation von Unix und Unix-ähnlichen Betriebssystemen** [Engl. für „Portable Operating System Interface"]
SH	**Schleswig-Holstein**
SMB	**Client-/Server-Protokoll** [Engl. für „Server Message Block"]
SWD	**Softwareinstallation** [Engl. für „Software Deployment"]
TPM	**Micro-Controller auf modernen Computern zur Erweiterung von Sicherheitsfunktionen** [Engl. für „Trusted Platfrom Module"]
UHD	**Anlaufstelle für Probleme, Störungen und Anfragen im IT-Bereich** [Engl. für „User Help Desk"]
UI	**Benutzerschnittstelle** [Engl. für „User Interface"]
UVgO	**Unterschwellenvergabeverordnung**
VLAN	**Virtuelles LAN** [Engl. für „Virtual Local Area Network"]
VPN	**Virtuelles Privates Netzwerk** [Engl. für „Virtual Private Network"]
WiBe	**Wirtschaftlichkeitsbetrachtung**
XML	**Textbasiertes Dateiformat** [Engl. für „eXtensible Markup Language"]
ZIT	**Zentrales IT-Management**

SH

Schleswig-Holstein
Ministerium für Energiewende,
Landwirtschaft, Umwelt, Natur
und Digitalisierung

Schleswig-Holstein. Der echte Norden.