

Mitglieder des Kreistags
des Landkreises Esslingen

Verwaltungs- und Finanz- 16.07.2026 öffentlich Kenntnisnahme
ausschuss

Betreff: Digitale Souveränität im Landratsamt Esslingen

Anlagen: Antrag Die Linke - Digitale Souveränität im Landkreis Esslingen

BESCHLUSSANTRAG:

Der Verwaltungs- und Finanzausschuss nimmt den Bericht zur digitalen Souveränität im Landratsamt Esslingen zur Kenntnis.

Auswirkungen auf den Haushalt:

Siehe Sachdarstellung.

Sachdarstellung:

Zum Antrag der Fraktion der Linken „Digitale Souveränität im Landkreis Esslingen“ vom 3. März 2026 hat die Verwaltung in der Sitzung des Verwaltungs- und Finanzausschusses (VFA) am 19. März zugesagt, in der Sondersitzung zum aktuellen Stand im Landratsamt zu berichten. Im Vorgriff auf die nachfolgenden Ausführungen sind die beantragten Punkte aus Sicht der Verwaltung bereits etabliert bzw. werden im Folgenden beantwortet.

I. Darstellung der aktuellen Digitalisierungsstrategie

Die Digitalisierungsstrategie des Landkreises Esslingen wurde zuletzt im September 2025 umfassend vorgestellt und im VFA präsentiert (Vorlage Nr. 094/2025). Aufbauend auf den vorangegangenen Bericht im Dezember 2023 (Vorlage Nr. 186/2023) wurden dabei insbesondere die erreichten Meilensteine und – zum Teil vorzeitig – abgeschlossenen Teilprojekte der Digitalisierungsstrategie I (2019 bis 2025) dargestellt. In Bezug auf die „Verantwortlichkeiten und Zuständigkeiten innerhalb der Verwaltung“ konnte berichtet werden, dass innerhalb des Dezernats 1 bereits im Jahr 2023 mit der Schaffung des Amt 15 „Informationstechnik und -sicherheit“ sowie des Sachgebiets 173 „Digitale Akte und Digitalisierung“ der wachsenden Komplexität der Aufgabe Rechnung getragen wurde. Ferner wurde die Digitalisierungsstrategie II (2025 bis 2030) vorgestellt. Diese wird von

den übergeordneten Hauptzielen einer „verlässlichen, bürgerfreundlichen und digital niederschwellig erreichbaren Verwaltung“ sowie von „durchgängig digitalen und teilweise automatisierten Verwaltungsprozesse (end-to-end-Digitalisierung), wo dies Effizienzgewinne ermöglicht,“ getragen. Ein Schwerpunkt ist hierbei die Einsatzmöglichkeit von KI und Automatisierung.

II. Digitale Souveränität im Landratsamt Esslingen

Vor dem Hintergrund des Antrags der Fraktion der Linken „Digitale Souveränität im Landkreis Esslingen“ wird im Folgenden eine gesonderte Betrachtung im Hinblick auf die Frage der digitalen Souveränität vorgelegt. Aufgrund des inhaltlichen Zusammenhanges werden die Fragen 2 und 3 entsprechend gemeinsam beantwortet.

1. Definition Digitale Souveränität

Der Begriff der Digitalen Souveränität bezeichnet im Kontext des Landratsamts die Fähigkeit einer öffentlichen Verwaltung über ihre eigenen digitalen Infrastrukturen, Daten und IT-Systeme selbstbestimmt, rechtssicher und unabhängig zu verfügen.

Dies umfasst drei wesentliche Kriterien:

- **Technologische Souveränität**
Dies bezeichnet die Kontrolle über die eingesetzte Hard- und Software sowie die Fähigkeit, Systeme eigenständig betreiben und anpassen zu können
- **Datensouveränität**
Kontrolle über Speicherort, Zugriff, Verarbeitung und Weitergabe aller verarbeiteten Daten.
- **Operative Handlungsfähigkeit**
Die Fähigkeit, alle Aufgaben auch im Falle externer Störungen, Vertragsänderungen oder politischer Einflussnahme wahrnehmen zu können.

Digitale Souveränität ist kein statischer Zustand, sondern ein kontinuierlicher Prozess der Risikobewertung, technologischen Weiterentwicklung und strategischen Planung. Sie bedeutet ausdrücklich nicht, auf alle externen Anbieter zu verzichten, sondern Abhängigkeiten bewusst zu steuern und auf ein kalkulierbares Maß zu begrenzen.

2. Rahmenbedingungen im Landratsamt Esslingen

Die Rahmenbedingungen zur Digitalen Souveränität rücken nicht zuletzt durch weltpolitische Entwicklungen immer mehr in den Fokus. Das Landratsamt verfolgt diese Entwicklungen und bettet diese in die laufende Fortentwicklung der Digitalisierungsstrategie ein. Ohne einen rechtlich festgesetzten Rahmen auf Bundes- oder Landesebene ist jedoch eine Festlegung auf einen eigenen, isolierten Weg des Landratsamtes höchst kritisch zu sehen. Vielmehr ist eine Verbundleistung der kommunalen Ebene im Zusammenschluss mit Land und Bund zwingende Voraussetzung.

2.1. Technische Abhängigkeit von Fachanwendungen

Das Landratsamt hat zahlreiche und unterschiedlichste Fachanwendungen, die zwingende Abhängigkeiten zu bestimmten Betriebs- oder Datenbanksystemen haben. Hierzu zählen nicht nur Anwendungen aus dem privaten Sektor, die speziell für den öffentlichen Sektor bereitgestellt werden, sondern auch Anwendungen, die von unserem Rechenzentrum (Komm.ONE) oder der Landesverwaltung bereitgestellt werden und genutzt werden müssen.

Einzelne Beispiele für eine zwingende Abhängigkeit insbesondere zu Microsoftbetriebssystemen sind:

- **Enaio:** Dokumenten-Management-System
- **Deviss / Schweb.Net (Nachfolgeverfahren):** Schwerbehindertenausweise
- **ESRI ArcGIS:** Erweiterung zur Erstellung der WebGIS Plattform
- **ProBauG:** Fachanwendung für das Baurechtswesen einschließlich dem digitalen Bauantrag

2.2. Rechtliche Rahmenbedingungen (Sicherheitsanforderungen)

Jede Entscheidung zur IT-Strategie des Landratsamts Esslingen wird im Kontext der geltenden Sicherheitsvorschriften bewertet. Die Zielsetzung der Sicherheitsvorschriften ist der Schutz der Informationen des Landratsamtes, wobei die Kernziele **Vertraulichkeit, Integrität und Verfügbarkeit** sind, die deckungsgleich Ziele der Digitalen Souveränität erfassen.

Das Landratsamt Esslingen ist seit Jahren bestrebt, die Informationssicherheit kontinuierlich zu verbessern. Unabhängig von externen Einflüssen ist die Verwaltung verpflichtet sicherzustellen, dass die Daten der Bürgerinnen und Bürger jederzeit geschützt sind und die Verwaltung ihre Dienst- und Betriebsfähigkeit aufrechterhalten kann. Hierzu zählen unter anderem die stetig wachsenden Anforderungen an die Informationssicherheit im Rahmen der Zusammenarbeit mit Bundes- und Landesbehörden.

Auf europäischer und Bundesebene wurde durch die Richtlinie NIS2 (EU 2022/2555), deren Umsetzung im aktualisierten BSIG, sowie durch das KRITIS-Dachgesetz ein neuer Gesetzesrahmen geschaffen, der die Anforderungen an die Informationssicherheit deutlicher formuliert und den Geltungsbereich gegenüber dem bisherigen Stand erheblich erweitert. Die Umsetzung der NIS2-Richtlinie auf die kommunale Ebene obliegt den jeweiligen Bundesländern. Das Land Baden-Württemberg verfolgt bislang den Ansatz, die kommunale Ebene auf freiwilliger Basis einzubeziehen. Daher ist die Kernverwaltung des Landkreises zunächst nicht unmittelbar betroffen. Gleichwohl ist seit Anfang 2024 die Siedlungsabfallbeseitigung im Rahmen der KRITIS Betrachtung von den erhöhten Anforderungen erfasst. Zunächst war allein die Kompostwerk Kirchheim unter Teck GmbH betroffen, seit Beginn des Jahres 2026 gilt dies auch für den Abfallwirtschaftsbetrieb des Landkreises. Aufgrund deren Vernetzung mit der Landkreisverwaltung im Rahmen verschiedener Verwaltungsleistungen strahlen die Anforderungen der genannten Gesetze mittelbar auf die Landkreisverwaltung aus. Dies umfasst insbesondere die sogenannten Risikomanagementmaßnahmen nach § 30 BSIG und die Meldepflichten nach § 32 BSIG.

Das **KRITIS-Dachgesetz** zielt insbesondere auf die Stärkung der physischen Resilienz von KRITIS Betrieben ab. Hierunter fallen beispielsweise Maßnahmen zum Perimeter-Schutz sowie zum Schutz vor Naturkatastrophen. Das Gesetz richtet sich an KRITIS Betriebe und ist damit unmittelbar für die Kompostwerk Kirchheim unter Teck GmbH relevant. Die Landkreisverwaltung selbst ist derzeit nicht direkt betroffen. Im Nachgang zur Gesetzgebung im März 2026 wurde verkündet, dass eine Ausweitung des Gesetzes innerhalb von spätestens zwei Jahren beabsichtigt ist. In welchem Umfang die Landkreisverwaltung sowie ihre Einrichtungen davon konkret betroffen sein werden, bleibt abzuwarten.

Für die Landkreisverwaltung und ihre Einrichtungen ergeben sich hierdurch (mittelbar) folgende Pflichten:

1. Konzepte in Bezug auf die Risikoanalyse und auf die Sicherheit in der Informationstechnik.
2. Bewältigung von Sicherheitsvorfällen,
3. Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement,
4. Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zu unmittelbaren Anbietern oder Diensteanbietern,
5. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen,
6. Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Sicherheit in der Informationstechnik,
7. Grundlegende Schulungen und Sensibilisierungsmaßnahmen im Bereich der Sicherheit in der Informationstechnik,
8. Konzepte und Prozesse für den Einsatz von kryptographischen Verfahren,
9. Erstellung von Konzepten für die Sicherheit des Personals, die Zugriffskontrolle und für die Verwaltung von IKT-Systemen, -Produkten und -Prozessen,
10. Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

3. Transparenz der Lizenzkosten

Zur Betrachtung der Rahmenbedingungen gehört die Betrachtung bestehender Lizenzverträge. Die im Antrag angedachte vollständige und detaillierte Übersicht sämtlicher Softwarelizenzen, einschließlich Laufzeit und Kündigungsfristen ist in der praktischen Umsetzung jedoch bei über 800 Verfahren mit erheblichem Aufwand verbunden. Zudem verändert sich die Anwendungslandschaft in der Verwaltung des Landkreises laufend und muss insbesondere durch Gesetzesänderungen regelmäßig angepasst und erweitert werden. Aus diesem Grund werden in Abstimmung mit der antragstellenden Fraktion nachfolgend die kostenintensivsten Verfahren (Planwerte 2027) aufgeschlüsselt.

Der jährliche Gesamtaufwand der kostenintensivsten Verfahren beläuft sich auf rund 4,04 Mio. EUR. Den mit rund 54 % größten Anteil bilden die Fachanwendungen der Komm.ONE (z. B. KM-Financen, KM-Personal, KM-Fahrzeuge, OWI 21, KM-Fahrerlaubnisse). Auf Microsoft entfallen rund 39 %. Hierauf entfällt allerdings zugleich die mit Abstand größte Zahl an Benutzerlizenzen (rund 2.200). Die Lizenz für das Landratsamt umfasst dabei einen deutlich größeren Funktionsumfang als eine reine Büroanwendung (vgl. Kapitel 4.1). Auf die digitale Akte entfallen bei rd. 1.030 Nutzenden rund 7 % der Gesamtaufwendungen.

4. Betrachtung der Microsoftlizenzen und alternativer Open-Source-Lösungen

Der Blick auf die Gesamtaufwendungen zeigt, dass die Kosten für die Nutzung von Microsoftanwendungen als Einzelposition einer der größten Kostenpunkte im Bereich der Lizenzverwaltung darstellen und gleichzeitig wird Microsoft in der öffentlichen Diskussion um die Abhängigkeit von nicht europäischen Softwareanbietern und Clouddiensten musterhaft regelmäßig erwähnt. Für das Verständnis der Position ist jedoch eine differenzierte Betrachtung und die Bedeutung der Microsoftumgebung für das Landratsamt vorzunehmen.

4.1. Zusammensetzung der Microsoftlizenzen

In der öffentlichen Diskussion wird Microsoft 365 häufig auf seine Office-Anwendungen (Word, Excel, Outlook, u.a.) reduziert. Dies entspricht nicht dem tatsächlichen Funktionsumfang einer M365 E5 Lizenz. Nachfolgend wird ein Überblick über die wesentlichen Leistungsbestandteile gegeben:

- **Produktivitätsanwendungen**
Word, Excel, Outlook, Onenote, Access, Publisher
- **Kommunikation & Kollaboration**
Microsoft Teams (Videokonferenz, Chat, Telefonie), SharePoint, Exchange Online
- **Identitäts- & Zugriffsmanagement**
EntraID, Mobile-Device-Management (Intune) Multi-Faktor-Authentifizierung, Privileged Identity Management, Conditional Access, Single-Sign-On
- **Informationsschutz & Compliance**
Audit-Looging, Compliance Manager für NIS2/DSGVO-Nachweise.
- **Erweiterte Bedrohungsabwehr**
Defender for Identity, Defender for Cloud Apps, Defender for Office, Defender for Server und Clients
- **Analyseplattform**
Power BI Pro, Business Intelligence und Berichtswesen
- **Automatisierung**
Power Automate, Power Apps: No-Code/Low-Code-Plattform

Das Landratsamt Esslingen würde durch einen Verzicht auf Microsoft 365 nicht lediglich Bürosoftware ersetzen müssen, sondern eine vollständig integrierte Sicherheits- und Verwaltungsplattform.

4.2. Einsatzszenario von Open-Source -Lösungen

Im vorangegangenen Abschnitt wurde dargelegt, dass die Microsoftumgebung ein Kernbestandteil einer integrierten Sicherheits- und Verwaltungsplattform bildet. Anhand dieses Beispiels können die Herausforderungen zu einer vollständigen Lösung von Microsoftdiensten dargestellt werden. Für den Ersatz der Microsoftumgebung muss in Teilen oder vollständig eine Vielzahl an Anwendungen von Verzeichnisdiensten oder Verwaltungsdiensten zur Installation oder Vorgabe von Sicherheitsrichtlinien über Antiviren oder Ransomwareschutz, hin zu Office Lösungen und Clouddiensten integriert und zusammengeführt werden. Dabei ist die Wirtschaftlichkeit einer solchen Umstellung komplex und nicht auf die Lizenzkosten zurückzuführen.

Eine Wirtschaftlichkeitsbetrachtung muss mindestens folgende Aspekte beinhalten:

- **Fachliche Eignung**
Die Open-Source-Lösung erfüllt die funktionalen Anforderungen vollständig oder mindestens in gleichwertiger Weise.
- **IT-Sicherheit**
Die Software wird aktiv gepflegt, erhält regelmäßige Sicherheitsupdates und ist durch anerkannte Stellen, z.B. BSI, bewertet.
- **Gesamtbetriebskosten**
Die Gesamtbetriebskosten einschließlich Einführung, Schulung, Support und Betrieb sind gegenüber vergleichbaren kommerziellen Lösungen konkurrenzfähig.
- **Wartbarkeit und Support**
Es existiert ein verlässlicher kommerzieller Support-Partner, der Service-Level-Vereinbarungen (SLA) verbindlich einhalten kann.

4.3. Bereits eingesetzte Open-Source-Software

Das Landratsamt Esslingen bekennt sich ausdrücklich zu Open-Source-Software und setzt diese bereits dort ein, wo die oben genannten Kriterien erfüllt sind.

Exemplarisch lassen sich die folgenden Beispiele nennen:

- Linux-basierte Server-Betriebssysteme
- Apache-Webserver und nginx für interne Webdienste
- PostgreSQL und MariaDB als Datenbankbackends für Webseiten
- Nextcloud-Instanz, einschließlich Nextcloud Office für die übergreifende Zusammenarbeit, sowohl intern als auch extern.

4.4. Lizenzverpflichtungen auch beim Einsatz von Open-Source-Lösungen

Wie bereits oben erläutert sind die Fachanwendungen häufig auf ein Betriebssystem festgelegt. Zudem greift das Landratsamt auch auf Server und Fachanwendungen in extern betriebenen Rechenzentren zu. Hierzu zählen zum Beispiel Fachanwendungen bei der Komm.ONE, der BitBW oder von privaten Anbietern. Solange diese Anwendungen eine Microsoftlizenzierung erfordern, ist in den meisten Fällen das Landratsamt verantwortlich diese Lizenzen einschließlich einer gültigen Software Assurance zu beschaffen und zu halten.

- **Zugriff auf Windowsserver (lokal, Komm.ONE oder in der Cloud)**
Windows Server Client Access Lizenz (CAL), je Nutzer oder Gerät, auch für Linux Clients verpflichtend
- **Zugriff auf gehostete Office Anwendungen**
Office CAL, je Nutzer oder Gerät
- **Nutzung von Microsoft Exchange**
Exchange Server CAL
- **Nutzung von Microsoft Teams**
Teams-Lizenz, unabhängig vom Betriebssystem des verwendeten Clients
- **Remote Desktop / Terminalserverzugriff**
Remote Desktop Services (RDS) CAL, auch für Linux-Clients erforderlich
- **Zugriff auf Microsoft SQL Server**
SQL Server CAL oder Core-Lizenz

Aufgrund der bestehenden Microsoftlizenzierung, einschließlich der benötigten Client Access-Licenses (CAL) und Software Assurance sind die oben genannten Lizenzanforderungen bereits abgedeckt.

5. Notwendigkeit globaler Technologieanbieter

Die Entwicklung von digitalen Technologien innerhalb Europas sind auf einzelne Anwendungsfälle begrenzt. In einigen Bereichen fehlen konkurrenzfähige Angebote, die auf europäische Lösungen zurückgehen. Die meisten umfassenden Lösungen stammen von amerikanischen Weltmarktführern und deren Konkurrenten. Beispielhaft hierfür stehen Microsoft, Cisco, Apple, Amazon (AWS) oder Alphabet. Im Bereich der mobilen Betriebssysteme für Smartphone und Tablets sind skalierbare, sichere und wartbare Lösungen auf dem Markt nicht verfügbar. Im Folgenden sind zwei Erwägungsgründe zu einer Strategie zur Digitalen Souveränität aufgezeigt.

5.1. IT-Sicherheit: Ressourcen und Reaktionsfähigkeit

Microsoft investiert nach öffentlich zugänglichen Berichten jährlich über 4 Mrd. US-Dollar in Cybersicherheitsforschung und beschäftigt mehr als 10.000 Sicherheitsspezialisten.

Diese Kapazitäten ermöglichen:

- Identifikation, Analyse und Behebung von Zero-Day-Schwachstellen innerhalb von Stunden bis wenigen Tagen
- Den Betrieb eines rund um die Uhr aktiven Security Operation Center mit weltweitem Bedrohungsmonitoring
- Kontinuierliche Weiterentwicklung KI-gestützter Sicherheitsmechanismen
- Koordination mit nationalen Sicherheitsbehörden bei kritischen Bedrohungslagen

Weder kommunal betriebene Open-Source-Systeme noch europäische Mittelstandsanbieter sind in der Lage, diese Kapazitäten auch nur annähernd bereitzustellen. Für eine Behörde wie das Landratsamt Esslingen, die NIS2- und KRITIS Anforderungen erfüllen muss, ist diese Sicherheitsinfrastruktur keine Option, sondern eine Notwendigkeit. Microsoft ist hier exemplarisch genannt und stellvertretend für weitere Anbieter, insbesondere im Bereich Sicherheit und Infrastruktur, wie Firewall- oder Netzwerklösungen, für die derzeit kein gleichwertiger europäischer Wettbewerber verfügbar ist.

5.2. Sicherheit der Mobilien Endgeräte

Im Landratsamt Esslingen werden als mobile Endgeräte ausschließlich Geräte der Firma Apple eingesetzt. Apple bietet als einzige kommerzielle Betriebssystemplattform eine durchgängige hardwarebasierte Sicherheitsarchitektur. Diese umfasst unter anderem eine Verschlüsselung auf Chip-Ebene, einen manipulationssicheren Bootprozess sowie eine nahtlose Integration in das Mobile Device Management. Für mobile Endgeräte im Außendienst existiert derzeit keine Open-Source-Alternative, die ein vergleichbares Sicherheitsniveau und gleichwertige Benutzerfreundlichkeit gewährleistet.

6. Datensouveränität und aktuelle Rechenzentrumsstrategie

Das Landratsamt Esslingen betreibt seine IT-Infrastruktur bereits nach dem Grundsatz der Datensouveränität:

- Alle produktiven Daten werden in zwei redundanten, getrennten und gespiegelten Rechenzentren vorgehalten. Beide Standorte befinden sich im Landkreis Esslingen. Darüber hinaus verfügt das Landratsamt Esslingen über ein weiteres Rechenzentrum für den Krisenfall (K-Fall).
- Soweit technisch möglich, werden alle Daten auf internen, durch das Landratsamt Esslingen betriebenen Speichersystemen gespiegelt vorgehalten. Eine unkontrollierte Speicherung in externe Cloud-Dienste findet nicht statt.
- Datensicherungen erfolgen nach dem 3-2-1 Prinzip, drei Kopien auf zwei verschiedenen Medientypen, davon eine Kopie außerhalb des Hauptstandorts (off-site). Die Produktivdaten des Landratsamts Esslingen werden auf hochverfügbaren Speichersystemen vorgehalten. Mittels Snapshot-Technologien werden in regelmäßigen Abständen lokale Sicherungen des Datenbestands erzeugt. Diese Sicherungen werden gemeinsam mit dem produktiven Datenbestand über ein zu diesem Zweck entwickeltes, proprietäres Protokoll, auf ein weiteres Speichersystem im K-Fall-Rechenzentrum repliziert.
- Um die Unabhängigkeit vom Hersteller der eingesetzten Speichersysteme zu wahren, erfolgt zusätzlich zu den genannten Snapshot- und Replikationsverfahren eine tägliche Sicherung des gesamten Datenbestandes auf einen durch das Landratsamt Esslingen betriebenen WORM-Speicher (Write Once Read Many).
- Der Zugriff auf diesen Speicher ist ausschließlich den Mitarbeitenden des Sachgebiets 153 „IT-Infrastruktur“ vorbehalten. Für jeden Administrator werden individuelle Zugangsdaten sowie eine Multi-Faktor-Authentifizierung eingesetzt.

- Eine Löschung der auf dem WORM-Speicher vorgehaltenen Backups ist technisch erst nach Ablauf der festgelegten Vorhaltezeit möglich.
- Die auf dem WORM-Speicher vorgehaltenen Backups werden unmittelbar vor ihrer Speicherung mithilfe des Verschlüsselungsalgorithmus AES-256-CBC verschlüsselt.
- Die initiale Implementierung sowie alle darauffolgenden Anpassungen am Backup-Konzept erfolgten nach den Vorgaben des BSI-Grundschutz-Bausteins CON.3 Datensicherungskonzept.
- Es erfolgt eine tägliche Sicherung der Daten, die innerhalb der genutzten Microsoft Cloud-Dienste gespeichert sind. Diese umfasst E-Mails (Exchange Online), persönliche und gemeinsame Dateien (OneDrive und SharePoint Online) sowie in Microsoft Teams gespeicherte Daten.
- Als Datensicherungsziel dient ein durch das Landratsamt Esslingen betriebenes Speichersystem.
- Im Rahmen dieser Sicherung wird, soweit technisch möglich, auf Dateiformate zurückgegriffen, die zusätzlich zu den Microsoft-eigenen Diensten eine Wiederherstellungsmöglichkeit auf alternative Plattformen unterstützen.
- Daten, die auf den Speichersystemen des Landratsamts Esslingen gespeichert sind, werden in Echtzeit im Hinblick auf bekannte Metadaten (z.B. Dateinamen) analysiert und mit bekannten Indikatoren für Ransomware-Aktivitäten abgeglichen. Wird dabei eine verdächtige Aktivität erkannt, erfolgt umgehend eine Isolierung des verursachenden Anwenders.

Der Aufbau des Rechenzentrums verdeutlicht, dass die Prinzipien der Digitalen Souveränität, explizit der Datensouveränität, von Beginn an mitgedacht werden.

7. Abschließende Bewertung

Das Landratsamt Esslingen bekennt sich ausdrücklich zum Einsatz von Open-Source-Lösungen und nutzt diese bereits proaktiv (unter anderem Linux-basierte Server, PostgreSQL- und MariaDB-Datenbanken, Apache- und nginx-Webserver sowie Nextcloud einschließlich Nextcloud Office). Open-Source-Lösungen werden überall dort eingesetzt, wo die definierten Kriterien der fachlichen Eignung, IT-Sicherheit, Wirtschaftlichkeit sowie Wartbarkeit und Support erfüllt sind. Ein pauschaler Verzicht auf kommerzielle Software ist jedoch weder rechtlich geboten noch technisch und wirtschaftlich sinnvoll umsetzbar.

Diesem stehen insbesondere folgende Gründe entgegen:

- **Technische Abhängigkeiten:** Zahlreiche Fachanwendungen, darunter das zentrale Dokumentenmanagementsystem enaio, ProBauG, Deviss/Schweb.Net und die WebGIS-Plattform, sind zwingend an Microsoft-Betriebssysteme gebunden. Auch bei einem Wechsel des Client-Betriebssystems bleiben Microsoft-Lizenzen für den Zugriff auf zentrale Server- und Rechenzentrumsdienste rechtlich verpflichtend.
- **Integrierte Sicherheitsplattform:** Microsoft 365 ist weit mehr als Bürosoftware. Die Plattform umfasst Identitäts- und Zugriffsmanagement, Multi-Faktor-Authentifizierung, erweiterte Bedrohungsabwehr und Compliance-Management. Ein Ersatz erforderte die Integration zahlreicher Einzellösungen ohne vergleichbare Gesamtdeckung.
- **Gesetzliche Anforderungen:** Durch die ausstrahlende Wirkung der NIS2-Umsetzung und des KRITIS-Dachgesetzes unterliegt das Landratsamt bereits heute erhöhten Sicherheitsanforderungen. Die Sicherheitsinfrastruktur globaler Anbieter,

mit milliardenschweren Investitionen in Cybersicherheit und rund um die Uhr betriebenen Security Operation Centers, ist durch kommunal betriebene Open-Source-Systeme derzeit nicht gleichwertig abbildbar.

- **Wirtschaftlichkeit und Akzeptanz:** Bisherige Prüfungen haben gezeigt, dass Open-Source-Lösungen in der Skalierung des Landratsamtes vergleichbare Kosten verursachen, teils funktionale Einschränkungen mit sich bringen und der notwendige Wissensaufbau sowie die Akzeptanzbildung bei Mitarbeitenden schwer kalkulierbare Risiken darstellen. Das Scheitern des LiMux-Projektes in München verdeutlicht diese Herausforderungen exemplarisch:
 - LiMux war eines der bekanntesten Open-Source-Vorhaben der öffentlichen Verwaltung in Deutschland. Die Stadt München stellte ab 2003 rund 15.000 Arbeitsplatzrechner auf ein eigenes Linux-System mit freier Bürossoftware um und galt lange als Vorzeigeprojekt für die Unabhängigkeit von kommerziellen Anbietern. 2017 beschloss der Stadtrat jedoch die Rückkehr zu Windows bis 2020, wegen hohem Pflegeaufwand im Parallelbetrieb, veralteter Software, Kompatibilitäts- und Akzeptanzproblemen. Die Kosten für die Rückmigration wurde seinerzeit auf rd. 90 Mio. EUR geschätzt.
- **Datensouveränität:** Mit zwei redundanten Rechenzentren im Landkreis, einem zusätzlichen K-Fall-Rechenzentrum, WORM-gesicherten und AES-verschlüsselten Backups sowie Echtzeit-Ransomware-Erkennung sind die Prinzipien der Datensouveränität bereits heute konsequent umgesetzt. Eine unkontrollierte Speicherung in externe Cloud-Dienste findet nicht statt.

Dieser bewährte Ansatz, gezielter Open-Source-Einsatz bei gleichzeitig bewusster Steuerung kommerzieller Abhängigkeiten, wird konsequent weiterverfolgt. Referenzprojekte wie die Stadt München oder in Frankreich bezüglich der eigenentwickelten Videokonferenzplattform „Visio“ werden dabei ebenso aufmerksam beobachtet wie europäische und bundesweite Initiativen zur Stärkung der Digitalen Souveränität.

Das Landratsamt begleitet diese Entwicklungen aktiv, gemeinsam mit dem kommunalen Rechenzentrum Komm.ONE und dem Landkreistag im Rahmen des Sprengels der IT-Leitungen. Gerade diese vernetzte Zusammenarbeit in den kreisübergreifenden Gremien des Landkreistags und der Komm.ONE sind aus Sicht der Verwaltung unerlässlich. Eine solche Entwicklung gelingt jedoch nur dann nachhaltig, wenn auch EU, Bund und Wirtschaft gemeinsam an einer europäischen Lösung interessiert sind und die dafür notwendigen Rahmenbedingungen, regulatorisch wie wirtschaftlich, aktiv gestalten.

Die Verwaltung wird die Kernaussagen dieser Vorlage im Rahmen der Sitzung präsentieren.

gez.
Marcel Musolf
Landrat