AARHUS UNIVERSITY

Digital Sovereignty

Security and privacy

EXAM fall 2025

Name	Initials	student number
Anonymous	xxx	xxxxxxxxx
Lecturer: Christian Damsgaard Jensen		

Due date: 11/12/2025

Contents

1 Executive Summary(Abstract)

The purpose of this report is to examine, expand and define the organizations current dependency on non-EU technology, evaluate the key risks associated with this direction, analyse and propose EU alternatives. The goal is to identify and map a road to digital Sovereignty.

The current political climate is quite inhospitable and it has become apparent that world leaders make drastic, snap decisions that brings large implication to the technological landscape, where big tech can be leveraged as political weapons, thus inherently changing the risk of reliance on such servies. Therefore companies, with suchs reliances, risks getting caught in the crossfire.

Services where there is a heavy reliance, from companies such a *Microsoft*, which hosts Azure Active directory (AD), used for identity management, *SharePoint* and *OneDrive*, which Lifeline Health Technologies(LHT) uses as a file sharing service, could suddenly become unavailable.

A loss of this service, which would be tantamount to loss of many years of technological IPs and achievements which could lead to unquantifiable damage to the company. Therefore, in this inclememt weather, a EU alternative for these servises, is quintessential.

The main findings of this report is an overreliance on:

- Microsoft Azure Services, where cloud hosting is indeterminate and jurisdictional expose is somewhat vague. Thus EU laws may be hard to apply.
- Process and regulatory mismatches - Data is easily given up to 3rd party cloud services or foreign governments, without regard for compliance (EU MDR)
- A thorough documentation is needed of other cloud solutions, specifically regarding SaaS tools.

Some of the main risks include:

- Overreliance on providers like microsoft Azure services.
- Unsupported operating systems such as Windows Server '12R2, SQL 2016, windows 7 and XP.
- Unmainted local VM's, tightly coupled to on-prem hardware og dongles.
- Unmainted network equipment.
- Poor physical access control.

Examples for some EU-alternatives :

- Univention - German based software for identity & access management. A self hosted AD, requiring a virtual machine. Can then handle all authentication, along with other features such as single sign-on(SSO) and multifactor authentication (MFA)
- Scaleway - A French based cloud provider, capable of hosting VM's for infrastructre purposes.
- KeyCloak - B2C IAM, which can be self hosted. Supporting OAuth2 and OpenID.

1.1 Overall Conclusion

This report supports the conclusion that an entirely new system, is recommended to be built up in parallel, to remove the heavy reliance on non-EU service providers. A gradual transition is adviced, but that is not in the scope of the report.

2 Introduction

This report addresses the current and ongoing challenges that is present within Lifeline Health Technologies ApS due to the merger between Mediscan ApS, an established manufacturor of ultrasound electronics equipment for the health industry. And HealthSync Mobile ApS (HSM), a younger, digital health oriented company. The two former companies originates from two different times, with differing missions and complex implementatitons.

The complexity created by thtis merger and associated difficulties, due to differing it-landscapes, has prompted the executive team, to commission this report to highlight, identify and analyse the requirements and dependencies, related to digital Sovereignty with a focus on non-EU providers. The purpose of this report therefore becomes to identify risks within the newly formed, yet disjointed, It invironment which LHT has inherited, with its included assets, and how dependencies has could cause problems regarding regulatory compliance, operation stability and long-term autonomy from non-EU actors.

The scope of this report covers the broader themes of digital Sovereignty, including identity and access management, data-storage, infrastructre and process mismatches, aswell as the risk associated with a futrure migration along with a focus on jurisdictional factors that arises when handling sensitive data or other regulated information.

The overall structure of this report is, an overview of the current technology and service landscape of LHT, and a accompanying dependancy analysis. These two tie into the risk assessment of the current status. This is followed by an evaluation of possible EU-alternatives to implemented services and comparison of the current implementatitoon. Lastly a recommended migration Strategy is proposed.

2.1 Abbreviations

Abbreviation	**Meaning**
LHT	lifeline health technologies
HSM	HealthSync mobile
AD	Active Active directory
MFA	multifactor authentication
GDPR	General Data Protection Regulation
EU MDR	european medical directive
B2C	Business to customer
XDR	extended detection reponse
SMB	Server message block
CI/CD	continuous integration / continuous deployment
SIEM	security information event monitoring

Table 1: Table of common abbreviations, used in this report

3 Current Technology and Service Landscape

As a result of the merger between Mediscan Aps and HealthSync Mobile Aps, the it environment, inherited to LHT, is comprised to two very different digital landscapes. These difference goes beyond mere technocal platforms, such as tool chosen for various tasks, but also divering filosophies. This leaves LHT to operation in a Hybrid environment, where some parts of the company use incompatible identity systems, inconsistent governance practices and service providers that might not be a perfect fit for EU regulations.

3.1 Mediscan technology landscape

Mediscan originates from traditional engineering practies, around product development, production, calibration and quality asurance. These include

- On-prem EU-local infrastructre, there the whole it system is segmented into various sub networks, for engineering, manufacturing and servers.
- Local AD controllers, running on older operating systems, with weak overall governance
- Weak network security regarding hardware, older switches with no updates
- No MFA and relying on password update rotations

The infrastructre inherited from Mediscan, shows strong prefence to local storage and authentication along with a typical product first approach, where cynersecurity is seen as a hinderance.

3.2 HealthSync Mobile's technology landscape

HSM oprates a rather modern techonology environment, based in the new cloud computing era. With a heavy reliance on popular service providers such as the Microsoft Azure suite, Google cloud and other Saas products. These include:

- An extensize implementation of Azure services such as: AD, kubernetes, Cosmos DB, PostgreSQL, Key Vault, Api management, blob storage and monitor + application insights.
- Heavy reliance on CI/CD pipelines and API updates, from non-EU cloud hosted services.
- JSON/WIRE-formatted data.
- Enforced MFA, and OAuth2 + OpenID for access to apps

HSM's modern Technology stack, which histroically has granted them the capability for rapid expansion and growth comes at the cost of strong ties to non-EU governed cloud services. Which could become subject to outside EU regulation.

3.3 The hybrid environment post merger

The post-merger leaves LHT with a partially integrated and partially improved hybrid network, currently consisting of:

- The legacy on-prem VLAN of Mediscan's solution for manufacturing and engineering
- HSM's Azure environment and dependencies
- Site-to-site VPN between the two company environments

Inconsistent and overlapping infrastructures creates uncertain flow between different parts of the company. This poses unknown and unmitigated risks, which could be leveraged as attack vectors and entry points.

3.4 Identity and Access management

An important integration issue is the overlapping domains, which results in some users need separate accounts to access multiple services. This leads to multiple services for the same purpose. This also introduces conflicting policies.

- Some users having multiple accounts, both on-prem and cloud.
- Azure AD policy, excludes the use of legacy hardware primarily found in Mediscan
- Inconsistent access rollout to internal file services such as Sharepoint.

Unnecessarily complicated access controls, which would require significant changes to the operation of the company infrastructre.

4 Dependency Analysis

4.1 Purpose

It is imperative that we're aware who our service providers are, this is to prevent certain types of attacks, such as those aimed at our supply chain. If we don't commit do out due diligence in vetting the providers, we are make ourselves vulnerable, which could undermine the efforts to ensure the safety of the company.

4.2 Dependency mapping

From the merger, HLS has inherited a multitude of dependencies. In the section below, the different types are listed:

4.2.1 A. Cloud infrastructre Dependencies

- Azure
  - Azure DevOps
  - Azure functions, to deploy custom script for legacy HL7 v2 conversion.
- Google Cloud services

4.2.2 B. Identity & Access management Dependencies

- Azure
  - Azure AD
  - Azure AD connect
  - Azure B2C
- On-prem AD

4.2.3 C. Application & SaaS Dependencies

- GitHub
- Microsoft Teams
- Slack

4.2.4 D. Security & Monitoring Dependencies

- Cisco
  - Cisco ASA firewall, last firmware update from 2020 - legacy
  - multiple managed Cisco ethernet switches
  - VPN - Cisco any connect.
  - VPN - Site-to-Site

4.2.5 E. Data processing & Clinical workflow Dependencies

- Azure
  - Azure Blob storage
  - Azure CosmosDB
- Custom solutions
  - C++ device-configuration tool(local)
  - HL7v2 to JSON translation scripts running in Azure functions
- Microsoft
  - OneDrive
  - SharePoint
- DICOM handling

4.2.6 F. Development and Tooling Dependencies

- GitHub
- Terraform

4.3 Current providers and dependency severity

Provider / Service	Jurisdiction	Area	Criticality	Sov. Risk	Lock-in
Microsoft Azure	US	Cloud compute/storage	High	High	High
Azure AD / B2C	US	Identity management	High	High	High
Microsoft 365	US	Collaboration & files	High	High	Medium
GitHub	US	Source code / CI	High	High	Low
Cisco ASA / VPN	US	Network perimeter	High	Medium	Medium
Cosmos DB	US	Clinical metadata	High	High	Medium
Azure Functions	US	HL7 ingestion	High	High	High
Slack	US	Communication (legacy)	Medium	Medium	Low
Google Cloud	US	Analytics / telemetry	Medium	High	Low
On-prem AD	EU	Manufacturing IAM	High	Low	High
Mediscan tools	EU	Device config	Medium	Low	High
AnyConnect VPN	US	Remote access	High	Medium	Medium

Table 2: Summary of current providers and sovereignty-related dependency severity.

In table: 2 the columns, *Criticality* refers to the company's current depency on the current implementation. *Sovereignty* Risk explains how much control the company loses over its assets, as they are hosted by these provices, and lastly *Lock-in* aims to indicate how difficult it would be to replace the service, if it was necessary.

5 Risk Assessment

To analyze how the digital soverignty is impacted LHT's inherited IT-environment, a risk assessment is carried out. It is done by using a impact-likelyhood matrix, seen on figure: 1. This model is comprised of nine sectons, each of a severity level, which ranges from low to critial. This is based on the likehood of occurence and the impact on the company, whether it be operational, legal or stategic.

The axis of the model are impact and likehood, where every step out of the axis increases in the steps, low, medium and high

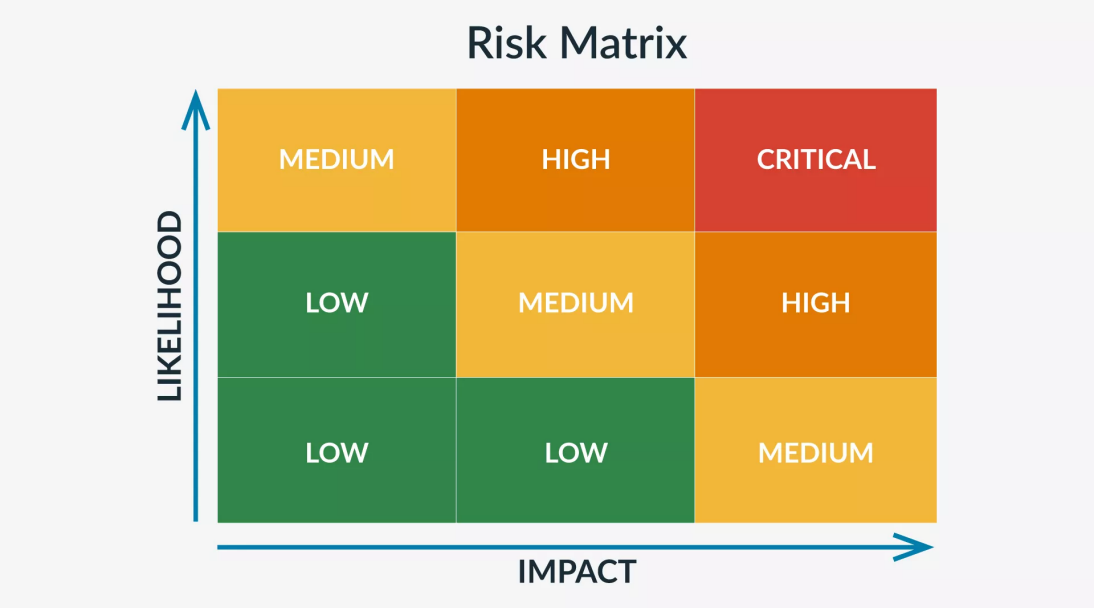

Figure 1: risk vs impact matrix, this is used to visually position LHT's risks. The The product of this matrix is indicated as *severity* in table 3, picture from AlertMedia: [1]

From this model it is possible to construct a table of the risks, pertaining to the current providers and dependency severity, found in table: 2, following the Methodology: $risk = Likelihood \cdot Impact$. The basis for this Methodology can be found at OWASP[2]. However in this case, likelyhood aims indicate how propable it is, that any impact on this dependency, will bring negative consequences for LHT as a whole.

Provider / Service	**Likelihood**	**Impact**	**Severity**	**Justification**
Microsoft Azure	LOW	HIGH	MEDIUM	Given the size of Microsoft. Constant resources are assigned to maintain Azure.
Azure AD / B2C	LOW	HIGH	MEDIUM	Same justification as Microsoft Azure.
Microsoft 365	MEDIUM	LOW	LOW	365 includes the office suite, thus they OutLook, where a lot of attack comes from phising.
GitHub	MEDIUM	MEDIUM	MEDIUM	The importance of GITHUB as a whole, makes it a desirable target.
Cisco ASA / VPN	HIGH	HIGH	CRITICAL	The Cisco switch has a known vulnerability , it sits on-prem and this could be exploted for confidential information.
Cosmos DB	LOW	HIGH	MEDIUM	This database contains sensitive information sent from device.
Azure Functions	LOW	HIGH	MEDIUM	Hals the upload of customer data and useage of custom function for HL7v2 translation.
Slack	MEDIUM	LOW	LOW	Should slack be compromised, it is merely an internal communcations channel. No information about sensitive company data being shared using Slack.
Google Cloud	LOW	LOW	LOW	Only historic use of this service, not noted as critical.
On-prem AD	HIGH	HIGH	CRITICAL	The likelyhood could be easily reduced by removing known firewall vulnerabilities.
Mediscan tools	HIGH	LOW	MEDIUM	Mediscan devices are in the hands of users. This increases the chances of exploits being exposed.
Site-to-site VPN	LOW	HIGH	MEDIUM	This is traffic on-prem to azure, if this is compromised, sensitive data can be accessed.

Table 3: Summary of current providers and sovereignty-related dependency severity.

Likelyhood can then further be broken down into questions like

- Likelihood of legal or jusrisdictional issues
- Likelihood of operational issues
- Likelihood of vulnerabilities regarding network security
- Likelihood of policy shifting

Given the overall dependency on software and services foreign to the EU, being mainly US based, and given current political climates. It becomes increasingly difficult to narrow down the probablity that foreign governments, might try to leverage services such as these, as political tools.

5.1 Regulatory Requirements for Health and Clinical Data

Because LHT is a producer of medical devices, that creates data which contains sensitive information about clients. This puts LHT in a position, where the data it possesses fall under GDPR[3]. This particular data falls under the special category data (Article 9), which requires the highest level of protection and oversight, with regards to processing, storage and transfer.
This introduces a particular risk when this data is being handled by non-EU cloud providers, such as Microsoft Azure. The ruling from Schrems II, states that: "Customers of US cloud service providers must now themselves verify the data protection laws of the recipient country, document its risk assessment and confer with its customers." - qouted from gdprsummary.com[4].
With this in mind, it becomes increasingly important for LHS to have complement control and Sovereignty, over the data created and stored.

5.2 Physical Vulnerabilities

5.2.1 Viby site

The Viby office, inherited from HSM, which implemented rather modern security practices. They rely mainly on Azure as their infrastructre environment, thus, does not indicate any significant physical security risk. However, since physical description of their offices has been supplied, it can only be assumed that they have implemened a minimum of physical office security. This includes thing like:

- No physical servers
- light network equipment, routers/firewall
- secured doors, with keycards
- auto-lock screensavers
- CCTV of building

It can only be assumed, due to the size and number of employees at HSM pre-merger, that the office was located in a shared-office building. This also points at things they most certainly didn't implement

- Biometric access
- Air-gapped security zones
- Cameras inside the offices
- Monitoring desk environments
- audit trails

These are things that more likely relate to ISO 27001[5], style physical access control, which, due to their environments and workflows, most likely didn't require.

5.2.2 Lystrup site

The Lystrup manufacturing site, inherited from Mediscan, with dedicated engineering and manufacturing environment, though it has been updated and improved over time. It still exposes several weakness, which has arisen from aging equipment.

- Basic server room with no biometric access, meaning anyone with a keycard can enter the room.
- Basic UPS with a ambient cooling and a mix of new and old equipment. No temperature monitoring of server equipment, impacts lifespan and reliability.
- Cisco ASA firewall, unpatched since 2020. This particular model of switch is vulnerable to a remote attack, which enables an attacker to gain memory content[6].
- legacy on-prem AD with no MFA, can be exploited to gain unrestricted access
- Physical access also allow the physical removal of decades of documentation, which could lead to IP theft.

5.3 How Identified Risks Impacts LHT's Digital Soverignty

The risks highlighted shows that the current landscape of LHT's sovereignty, is primarily dictated by foreign, non-EU cload platforms, which includes a wide span of roles and services. From the development environments, to azure AD and data processing, because these are US based companies, they have to comply with legislation, such as the CLOUD act[7] and FISA_702[8], this means that LHT does not fully control who gets access to data. And that this data can be accessed and requested by foreign governments.

In addition to this, many of these non-EU services has a high degree of vender lock-in, particularly, in this azure, that contains servers for both authentication, identity management, data ingestion and processing. This severely hampers the autonomy of LHT and its ability to restructure the organization in the future.

The current physical vulnerabilities of the company, which is primarily found in the engineering and manufacturing side of the organization, is affected by weak physical access controls, aging or degrading hardware and legacy software dependancies. This contributes an overall security risk.

6 EU-Alternatives

To strenghten digital Sovereignty, it is imperative that services gets migrated to EU friendly alternatives. To do this, the requirements can be broken down into different functional areas. Where each area is corresponds to a dependency.

- Identity & Access Management - The focus here is employeee authentication and identity MFA, employee and customer identity management with AD features
- Cloud compute & Hosting - To replace services currently held by Azure, which includes API hosting, data ingestion, functions and kubernetes like features
- Data Storage & processing - Azure blob and CosmosDB, currently handle critical functions such as HL7v2 conversion, DICOM data uploads. Alternatives should have physical address in the EU, with strong encryption
- Development & DevOps - This should include services with the ability to host source, CI/CD pipeline, issue tracking, version control and support GIT based workflow.
- Collaboration & Productivity tools - To replace service commonly provided by Microsoft. Services here are email, documents, internal communication, file storage and file sharing.
- Security & Monitoring - A replacement for Cisco products, should be able to prove services such as VPN, SIEM, logging and zero-trust capabilites.
- Patient/customer identity - A replacement for Azure B2C, which handles App user accounts and authentication. Must be able to be integrated into applications.

- Legacy On-prem Replacement & Hybrid Integration - Current setup implements physical SQL servers, legacy SMB shares and physical AD. The AD should be integrated with the IAM service, and legacy servers should be integrated into a single physical setup with a cloud backup, along with tightened physical security access.

With all the functional areas, which LHT relies on, outlined the next step is identify and pick european service providers, who can satisfy the different requirements. In order to minimize risk and impact, solutions who implement multiple services into a single provider, such a Azure does, is preferable, however this also brings some of the vendor lock-in back into the equation.

European alternatives are listed below,

- Identity & Access Management - Univention[9], a German based IAM solution, that can handle AD, and their IAM service NUBUS[14].
- Cloud compute & Hosting - Scaleway[10], a French based cloud compute company, which includes virtual machines and kubernetes abilities. With data residency inside european borders.
- Data Storage & processing - This requirement can also be delivered by Scaleway, as they also provide object storage of large amounts of data aswell as block storage.
- Development & DevOps - general CI/CD operations can be hosted in a GIT server, hosted by Scaleway.
- Collaboration & Productivity tools - LibreOffice[11] is an latvian alternative to the Microsoft office suite. As for collaboration tools, NextCloud, which originates from Germany.
- Security & Monitoring - WithSecure[12] from Finland, An XDR solution is chosen, because the necessty of more than just an antivirus at enterprise level is required. Along with LogPoint[13], a Danish company, which is a SIEM solution, which is an information correlation service.
- Patient/Customer identity - Univention's NUBUS has an integration with KeyCloak[15], which is open-source, that supports OpenID and OAuth2. Which can be self hosted.
- Legacy On-prem Replacement & Hybrid Integration - The hardware server offings in europe, is still in its infancy, a japanese alternative from Fujitsu[16] could be considered.

These proposed solutions and how they stack up against the current implementation will be discussed in the next sectiton.

7 Comparison of current and proposed solutions

The Suitablility of these EU derived alternatives will here be evaulated against the already implemented solution, in terms of technical compatability, which reflects how well this solution fits into the current LHT environment.

Technical compatability assesses the difficulty of implementing the proposed solutions, into the environment of LHT. Replacing all Azure services and with suitable replacements, which offers equivalent services, in this case Univention for identity management and Scaleway for hosting for cloud computte and storage, reduces the implementation effort, thus increases the chance of a smooth migration

Examples of this is the Active directory from Univention, which replaces Azure AD, with minimal changes to already implemented authentication dependencies. Univention also provides NUBUS with keyCloak, which preserves the use of OAuth2 and OpenID for customer usageage. While changing the underlying structure to a self-hosted environment, located in the EU.

Distributing the services across a number of different EU providers, increases the flexibility and should reduce the long term vendor lock-in. An example of this is ScaleWay, which can do both cloud compute, data storage and processing. But also host a GIT server and other required developer tooling, but with smaller requirements for future changes.

8 Conclusion

If this change in infrastructre is implemented, it would increase the digital sovereignty of the company and decrease its reliance on American services. In the risk analysis, it became apparent that both companies of this merger, were stuck in two different infrastructe and culture ideologies. Mediscan, being a product development company, with firm roots in engineering practicies and bandaid solutions and HealthSync Mobile, a more contemporary company, whose development pratices better reflect, the modern environment of cloud companies.
To intertwine the two companies and their ecosystems, with impunity, taking their current infrastructures into account, seems almost like wishful thinking. With the current geopolitical situation, a completly new and revised structure of the entire IT system is preferable. The transition should preferably be gradual, both to support cultural changes, for both agile developers and seasoned engineers, along with strong customer support to guide them through the transition, should any unforseen circumstances arise.

References

[1] AlertMedia. *What is a Risk Matrix how to use in your business*. 2025. URL: https://www.alertmedia.com/blog/risk-matrix/ (visited on 12/11/2025).

[2] OWASP. *OWASP Risk Rating Methodology*. 2025. URL: https://owasp.org/www-community/OWASP_Risk_Rating_Methodology (visited on 12/10/2025).

[3] Intersoft consulting. *Art. 9 GDPR, Processing of special categories of personal data*. 2025. URL: https://gdpr-info.eu/art-9-gdpr/ (visited on 12/11/2025).

[4] GDPR Summary. *Schrems II a summary - all you need to know*. 2025. URL: https://www.gdprsummary.com/schrems-ii// (visited on 12/11/2025).

[5] www.iso.org. *ISO/IEC 27001:2022*. 2025. URL: https://www.iso.org/standard/27001 (visited on 12/11/2025).

[6] sec.cloudapps.cisco.com. *Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software Web Services Information Disclosure Vulnerability*. 2025. URL: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-info-disclose-9eJtycMB (visited on 12/11/2025).

[7] Government of the United States. *CLOUD Act*. 2025. URL: https://www.justice.gov/criminal/cloud-act-resources (visited on 12/11/2025).

[8] Government of the United States. *Foreign Intelligence Surveillance Act, FISA section 702*. 2025. URL: https://www.intel.gov/foreign-intelligence-surveillance-act/fisa-section-702 (visited on 12/11/2025).

[9] Univention. *Univention*. 2025. URL: https://www.univention.com/ (visited on 12/11/2025).

[10] Scaleway. *Scaleway products*. 2025. URL: https://www.scaleway.com/en/all-products/ (visited on 12/11/2025).

[11] libreoffice. *libreoffice*. 2025. URL: https://www.collaboraonline.com/based-on-libreoffice/ (visited on 12/11/2025).

[12] WITHSECURE. *why withsecure*. 2025. URL: https://www.withsecure.com/why-withsecure/ (visited on 12/11/2025).

[13] logpoint. *SIEM logpoint*. 2025. URL: https://logpoint.com/en/product/siem/ (visited on 12/11/2025).

[14] Univention NUBUS. *NUBUS - Central identity and Access Management*. 2025. URL: https://www.univention.com/products/nubus/ (visited on 12/11/2025).

[15] Univention. *Navigating the Keycloak Admin Console with Nubus: A Step-by-Step Introduction*. 2025. URL: https://www.univention.com/blog-en/2024/10/navigating-the-keycloak-admin-console/ (visited on 12/11/2025).

[16] FUJITSU. *PRIMERGY Servers*. 2025. URL: https://www.fujitsu.com/global/products/computing/servers/primergy/index.html (visited on 12/11/2025).