TeleTrusT Information Security Professional

TeleTrusT Professional for Secure Software Engineering

EDV-Unternehmensberatung Floß GmbH

as-s3c

T.I.S.P./T.P.S.S.E. Community Meeting 2025

Berlin, 04. - 05.11.2025

(Ein) Der Weg in die sichere und souveräne MS365 Welt

Thomas Floß, EDV-Unternehmensberatung Floß GmbH

Frank Mördel, as-s3c GmbH

Ihr Referent

EDV-Unternehmensberatung Floß GmbH

Thomas Floß

EDV-Unternehmensberatung Floß GmbH

- geprüfter Datenschutzbeauftragter (TÜV / udis)
- Teletrust Information Security Professional (T.I.S.P.)
- geprüfter EDV-Sachverständiger
- Certified Ethical Hacker (CEH)
- IT-Forensiker
- geprüfter IT-Compliance Officer (TÜV)
- Certified Information Systems Auditor (CISA)
- Certified Data Privacy Solutions Engineer (CDPSE)
- Ausbilder für den technischen Datenschutz (udis gGmbH)
- Ehrenamtlicher Richter am Landgericht Bielefeld

Ihr Referent

Frank Mördel

AS-S3C GmbH

- Wirtschaftsinformatiker
- IT-Sicherheitsbeauftragter TÜV
- Certified Ethical Hacker (CEH)
- compTIA security+
- PTS (Penetration Testing Specialist (CertPro)
- BSI -Grundschutzpraktiker, -Vorfall-Experte und -Digitaler Ersthelfer
- Security Consultant & Trainer

Kompetenzen

- **BSI-Grundschutz**
- **IT-Sicherheit, Strategie & Compliance**
- **IT-Infrastruktur, Konzeption, Netzsegmentierung, Automatisierung**
- **Ethical Hacking / Pentesting**
- **IT-Virtualisierung**
- **Rechenzentrum Aufbau & Betrieb**

EDV-Unternehmensberatung
Floß GmbH

as-s3c®

Agenda

- Herausforderungen 2024, EOL Sharepoint, Exchange & Co.
- Technisches Umfeld
- Lösungsideen
- Der Weg in die Cloud
- Lösung für den rechtskonformen Einsatz der M365 Welt
- Was noch wichtig, aber nicht schwer ist

EDV-Unternehmensberatung
Floß GmbH

as-s3c®

Herausforderungen Anfang 2024
EOL Sharepoint, Exchange & Co.

Herausforderungen Anfang 2024

EDV-Unternehmensberatung Floß GmbH

as-s3c®

Microsoft Exchange 2016 ist End of Life (EOL)

Microsoft Sharepoint 2016 ist EOL

Windows Server 2016 Systeme und Windows 10 Systeme sind EOL

Sicherheitsupdates für die den Exchange & die Windows Server Systeme werden durch den Dienstleister nicht in der gewünschten Geschwindigkeit eingespielt (Personalverfügbarkeit wie auch Qualität)

Microsoft 365 Lizenzen sind vorhanden, werden aber nicht optimal genutzt

Herausforderungen Anfang 2024

EDV-Unternehmensberatung Floß GmbH

as-s3c®

Bei fast allen Microsoftprodukten ist somit der EOL für 2025 definiert und

- keine „normalen“ Lizenzen mehr erhältlich (Sharepoint, Exchange)
  - Alternative: Subscription Edition Sharepoint & Exchange
- Windows-AD nicht auf dem allerneusten Stand
- Anbindung an die Entra-ID (hier nur Teams) nur halbherzig umgesetzt

Diese Herausforderungen haben (hatten) tausende von KMU‘s in Deutschland

EDV-Unternehmensberatung
Floß GmbH

as-s3c®

Technisches Umfeld

Technisches Umfeld

EDV-Unternehmensberatung Floß GmbH

as-s3c®

Ausstattung in der Company (14 Arbeitsplätze)

- Clients: Apple Macintosh Systeme, alles auf dem (fast) neusten Stand
- 5 Windowssysteme (Windows 10) als virtuelle Systeme für die Anwendungen, die nicht auf dem Mac verfügbar sind
- Synology NAS Systeme, eingebunden in die AD
- Nextcloud (lokal gehostet)
- Serverlandschaft (virtuell)
  - Windows 2016 (2 x AD-Server)
  - Sharepoint 2016
  - Exchange 2016

Technisches Umfeld

EDV-Unternehmensberatung Floß GmbH

as-s3c®

- Office 365 Lizenzen vorhanden (M365 Standard)
- Alle primären Anwendungen laufen DSGVO konform in der Cloud
  - Stackfield (Aufgabentool) → vollständige Verschlüsselung
  - Stashcat (Messenger) → vollständige Verschlüsselung
  - Weclapp (ERP System)
  - DATEV (Buchhaltung & Co.)
  - Starface (Telefonie)
  - Timebuttler, Mite (Zeit-/Projektzeiterfassung)
  - ….

zu allen Anwendungen sind AV-Verträge vorhanden, ausser MS alles deutsche Anbieter

EDV-Unternehmensberatung
Floß GmbH

as-s3c®

So, oder so ähnlich, geht es ca. 80% des Mittelstandes!

Aber was machen?

EDV-Unternehmensberatung
Floß GmbH

as-s3c®

Lösungsideen

EDV-Unternehmensberatung
Floß GmbH

as-s3c®

Lösungsideen

Umzug in die Cloud mit folgenden Vorgaben:

- Sicherer RZ Betrieb
- 24x7x365 Support
- Schnelles Patching & fortlaufende Überwachung (Reaktionszeiten)
- Tools zur sicheren Konfiguration der Umgebung (z.B. Conditional Access)

- Datenhoheit bleibt im eigenen Unternehmen (Verschlüsselung)
- Im Ernstfalle Rückzug aus der Cloud binnen 2-4 Tagen

- Dienstleister die etwas von Sicherheit verstehen

Lösungsideen

EDV-Unternehmensberatung Floß GmbH

as-s3c

M365 wurde somit erste Wahl, insbesondere wegen dem Sharepoint. Aber, wie bekommt man den Cloud- und FISA-Act in den Griff?

Lösung: Verschlüsselung der Daten, aber unter eigener Souveränität

Aber wie? Cryptomator und Co. sind für Einzelplatzuser und nicht (kaum) für eine Company geeignet!

ABER, 2020 war beim Teletrust Innovationspreis ein Hersteller dabei, der eine eigene Verschlüsselung u.A. für die M365 Welt im „Angebot“ hatte → eperi!

Lösungsideen

EDV-Unternehmensberatung Floß GmbH

as-s3c®

Somit war der Weg vorgegeben, der die Sicherheitsvorgaben erfüllt!

Dieses gilt auch für die **DSGVO** etc., denn eine richtige Verschlüsselung unter eigener Flagge löst die rechtliche Problematik zu (fast) 100%.

Weiterhin lösen wir fast alle Herausforderungen rund um die die NIS 2 – Richtlinie, der ISO27001, der TISAX, …. die da wären:

- Wahrung der Vertraulichkeit
- Höchste Verfügbarkeit
- Wahrung der Integrität

Lösungsideen

EDV-Unternehmensberatung Floß GmbH

as-s3c®

Jetzt war zu klären wie und mit wem können die nötigen Schritte (Verschlüsselung, sicherer Tenant, …) umgesetzt werden und wie sieht die Kostenstruktur aus?

Denn, warum etwas Neues suchen, testen und implementieren, wenn alle geforderten Punkte doch schon in vorhandenen Cloudsystemen (z.B. M365, Google, AWS) gegeben sind?

EDV-Unternehmensberatung
Floß GmbH

as-s3c®

Der Weg in die sichere und DSGVO konforme Cloud am Beispiel von M365

Der Weg in die Cloud

EDV-Unternehmensberatung Floß GmbH

as-s3c®

Claudia Plattner, Präsidentin BSI

…. deshalb brauche es einen strategischen Ansatz, der folgende Fragen beantworte:

1. Welche digitalen Technologien wollen wir einfach einkaufen und „out of the box“ verwenden?

Der Weg in die Cloud

EDV-Unternehmensberatung Floß GmbH

as-s3c®

Claudia Plattner, Präsidentin BSI

2. Für welche digitalen Technologien streben wir für Teile der digitalen Wertschöpfungskette die globale Exzellenz aus nationaler und europäischer Hand an?

3. Welches sind die außereuropäischen Technologien, die wir (vorerst) weiterverwenden und die vorab technisch so abgesichert und veredelt werden können, dass die Kontrolle über Daten und Steuerung bei uns liegt?

…….

Der Weg in die Cloud

EDV-Unternehmensberatung Floß GmbH

as-s3c®

Stichworte sind dabei u.a.:

- **Verschlüsselung**
- Klassifizierung
- **Risikoanalyse**
- **richtige Konfiguration**
- **klare Richtlinien und Vorgaben**
- … alles auch Normenanforderungen sowie der NIS 2 Umsetzung

Der Weg in die Cloud

EDV-Unternehmensberatung Floß GmbH

as-s3c®

Doch was sagen die „Anderen“?

- In die M365 Welt? Dass ist doch nicht sicher und schon gar nicht DSGVO konform.
- Keine Datensouveränität ….
- Die Aufsichtsbehörden sagen doch dass das (überhaupt) nicht geht.
- Juristisch ist das nicht umsetzbar, die Verträge mit MS sind nicht „sauber“

Der Weg in die Cloud

EDV-Unternehmensberatung Floß GmbH

as-s3c®

- **Wie steht es mit der Sicherheit in der M365 Welt?**

➢ Einer neuer Tenant hat standardmäßig wenig/nicht alle erforderlichen Sicherheits- wie Datenschutzeinstellungen

➢ In den „kleinen“ Lizenzpaketen gibt es wenige / keine Sicherheitstools (Defender, Intune, etc.)

→ Microsoft (aber alle anderen auch) lässt sich Sicherheit bezahlen

➢ Telemetriedaten ausschalten!

Der Weg in die Cloud

EDV-Unternehmensberatung Floß GmbH

as-s3c®

- **E5, die Lizenz mit Verschlüsselungsmöglichkeit**

➢Kunden haben zwei Optionen für die Verwaltung von Verschlüsselungsschlüsseln auf Dienstebene:

– Von Microsoft verwaltete Schlüssel
In der Standardimplementierung für Kunden, die keinen Kundenschlüssel verwenden, verwaltet Microsoft alle für die Dienstverschlüsselung verwendeten kryptografischen Schlüssel. Diese Option ist zurzeit standardmäßig für Exchange Online, SharePoint Online und OneDrive for Business aktiviert. Von Microsoft verwaltete Schlüssel bieten eine Standarddienstverschlüsselung, es sei denn, ein Kunde macht ein Onboarding auf Kundenschlüssel.

Quelle: Microsoft

Der Weg in die Cloud

EDV-Unternehmensberatung Floß GmbH

as-s3c®

- **E5, die Lizenz mit Verschlüsselungsmöglichkeit**

  – Kundenschlüssel
  Mit dieser Option können Kunden ihre eigenen Stammschlüssel zum Verschlüsseln von Kundendaten verwenden. Kundenschlüssel werden in Azure Key Vault hochgeladen oder darin generiert, sodass Kunden die Fähigkeit von Microsoft-Diensten steuern können, Kundendaten zu entschlüsseln und zu verarbeiten. Diese Option ist zurzeit in Exchange Online, SharePoint Online und OneDrive for Business verfügbar.

Quelle: Microsoft

Der Weg in die Cloud

EDV-Unternehmensberatung Floß GmbH

as-s3c®

Fazit:

Einer neuer Tenant hat standardmäßig nur eine mittlere Sicherheit.

Die „kleinen“ Pakte beinhalten keine „wirkliche“ Verschlüsslung.

Beim großen Paket (E5) verwaltet Microsoft die Schlüssel.
Das ist, als wenn der Haustürschlüssel unter der Fußmatte liegt!

Wird die Microsoft Verschlüsselung genutzt, so funktionieren nicht alle Dienste uneingeschränkt.

Der Weg in die Cloud

EDV-Unternehmensberatung Floß GmbH

as-s3c®

Fazit:

Einer neuer Tenant hat standardmäßig nur eine mittlere Sicherheit.

Die „kleinen“ Pakte beinhalten keine „wirkliche“ Verschlüsslung.

Beim großen Paket (E5) verwaltet Microsoft die Schlüssel.
Das ist, als wenn der Haustürschlüssel unter der Fußmatte liegt!

Somit ist die Microsoft eigene Verschlüsselung NICHT die Lösung!

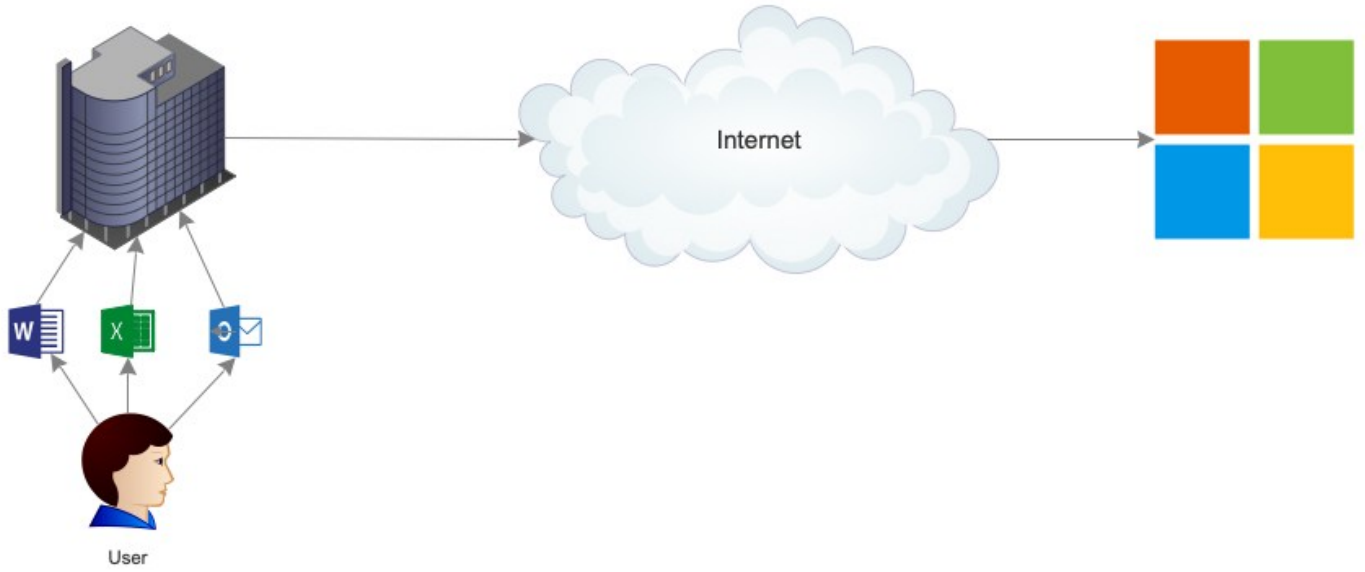
EDV-Unternehmensberatung
Floß GmbH

as-s3c®

Lösung für einen rechtskonformen Einsatz der M365 Welt

Lösung

Der Standardzugriff in die M365 Welt

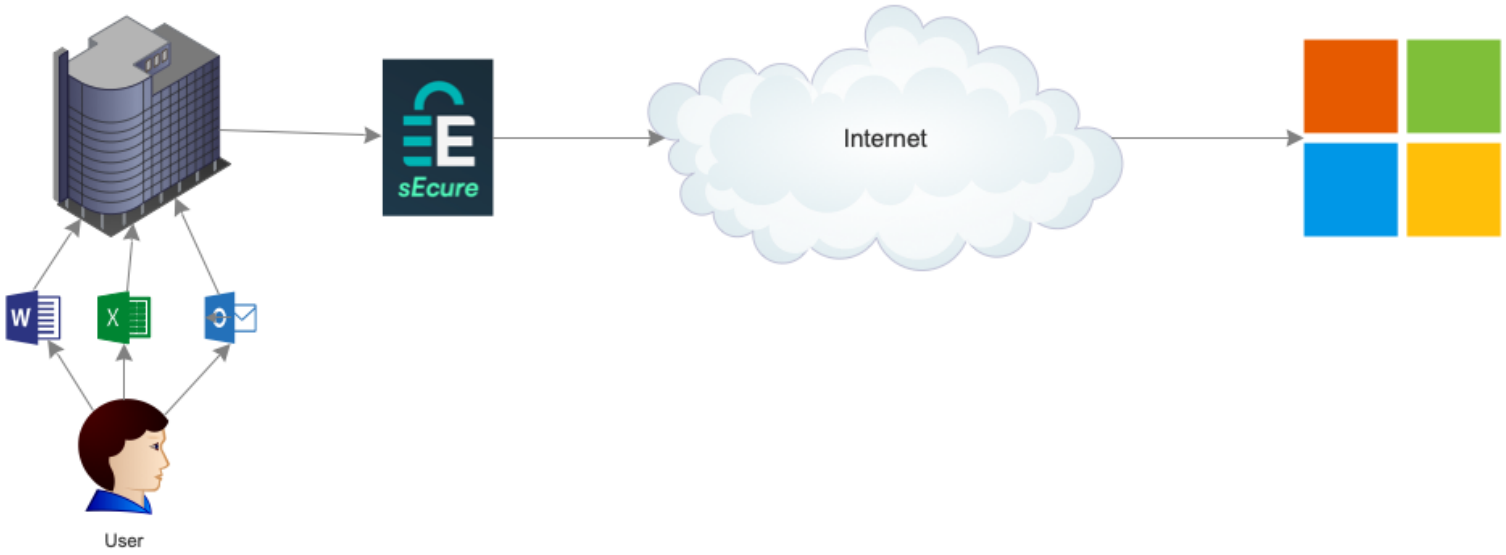


Lösung

EDV-Unternehmensberatung Floß GmbH

as-s3c®

Der DSGVO konforme Zugriff in die M365 Welt

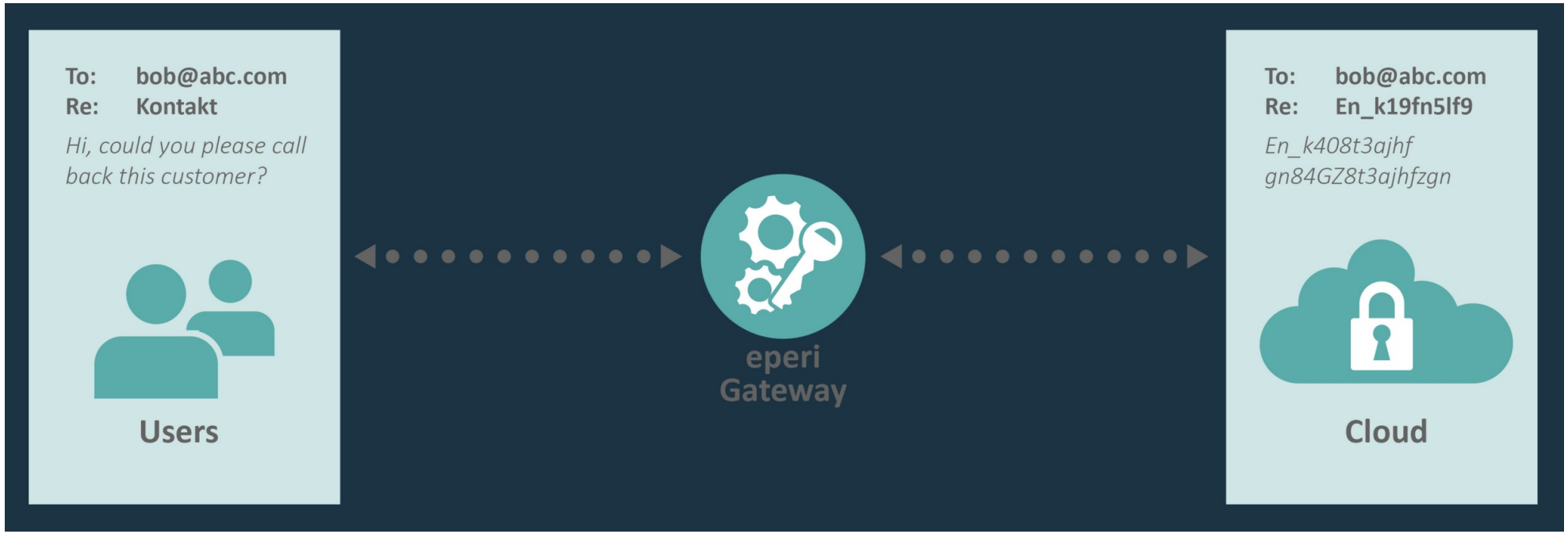


Lösung

EDV-Unternehmensberatung Floß GmbH

as-s3c®

- Es muss eine eigene Verschlüsselung her, entweder im eigenen Serverraum oder in einem deutschen RZ betrieben.



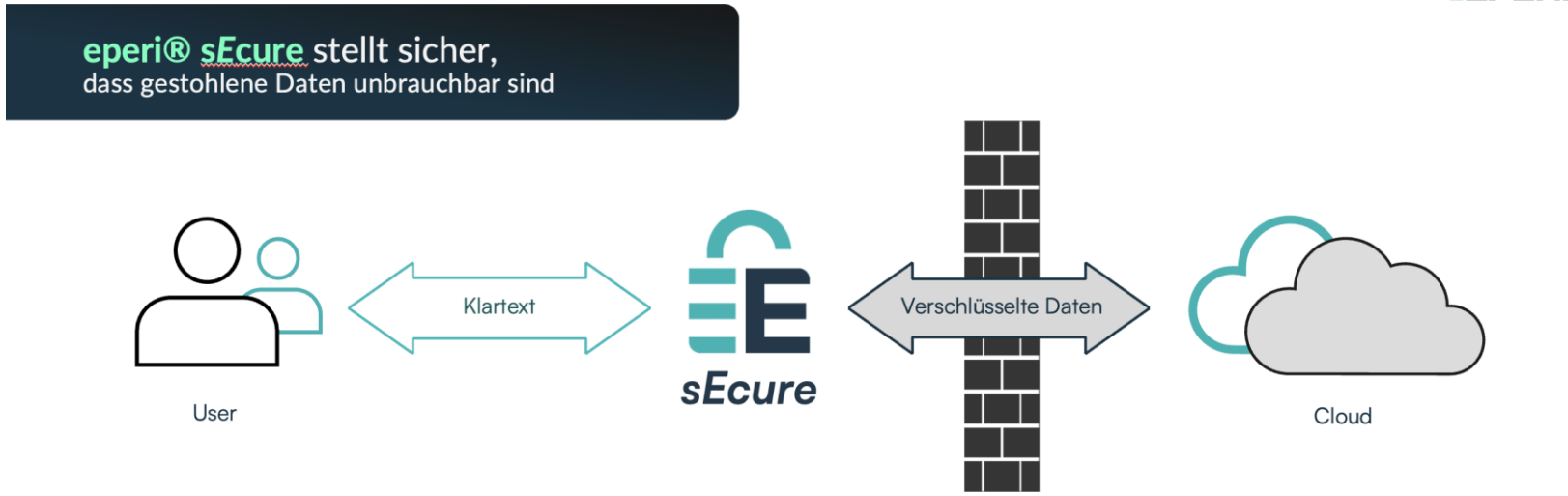
Lösung

EDV-Unternehmensberatung Floß GmbH

as-s3c®

- Es muss eine eigene Verschlüsselung her, entweder im eigenen Serverraum oder in einem deutschen RZ betrieben.

EPERI

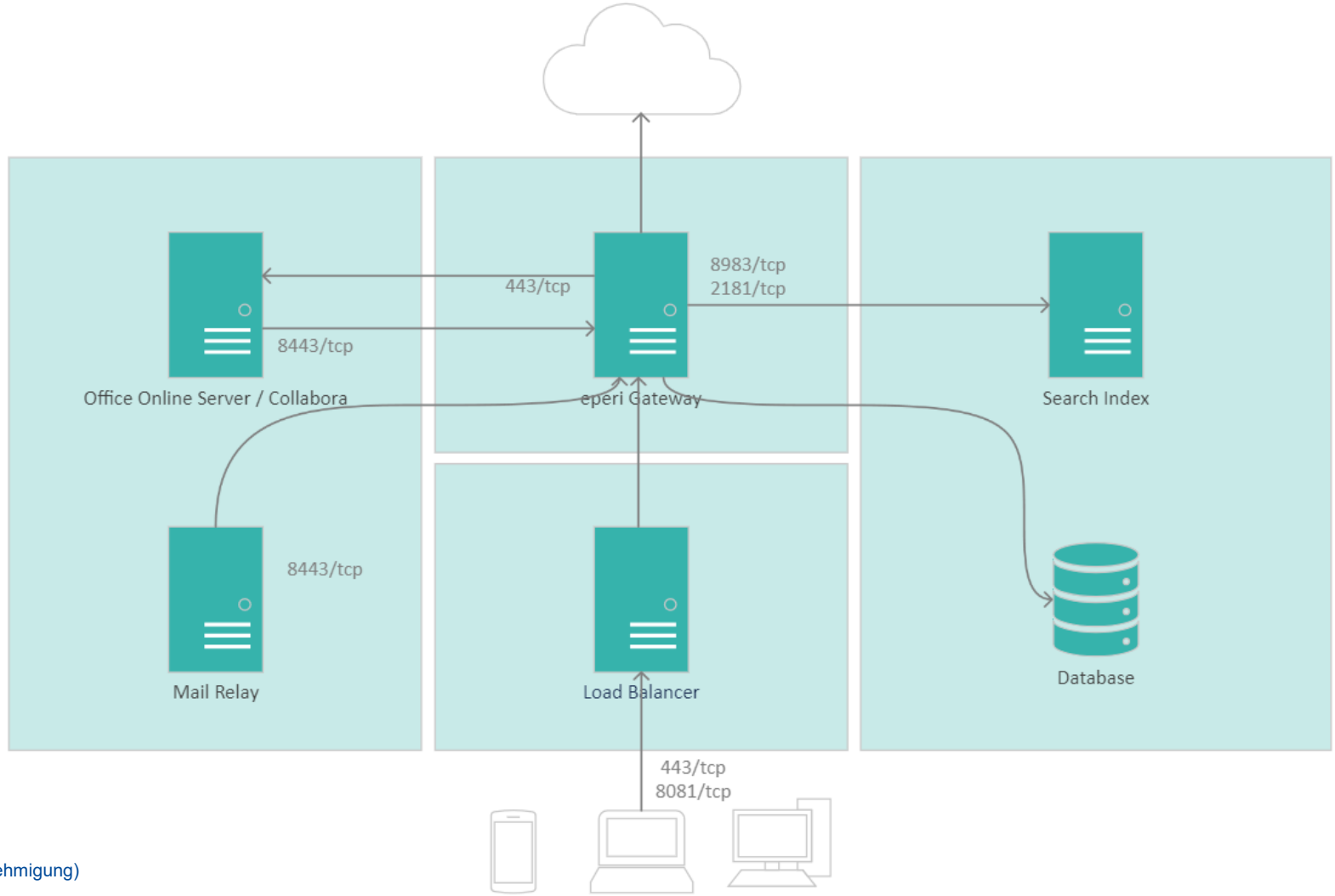


Lösung

EDV-Unternehmensberatung Floß GmbH

as-s3c®

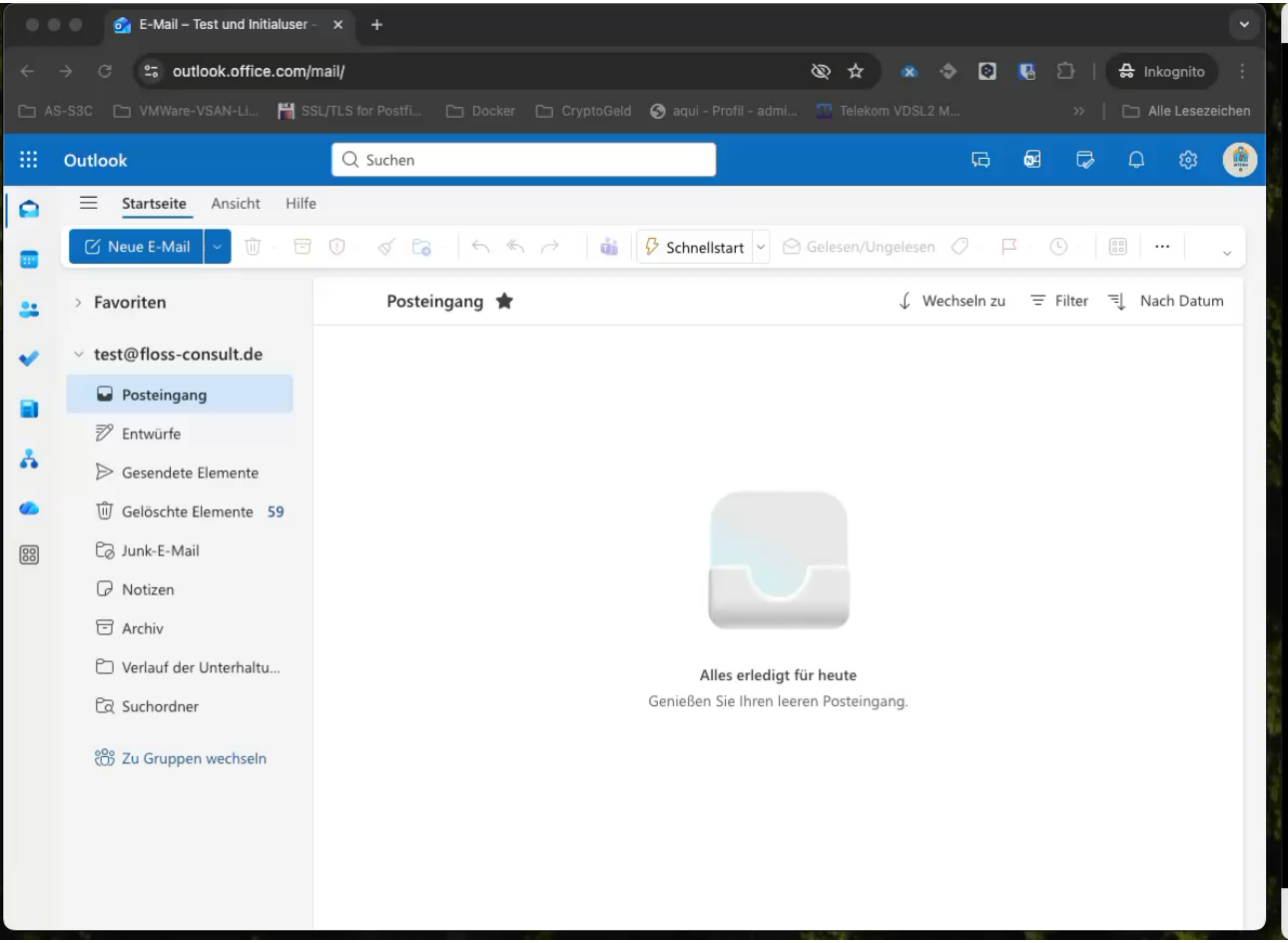
„Richtige“ Verschlüsselung am Beispiel eperi

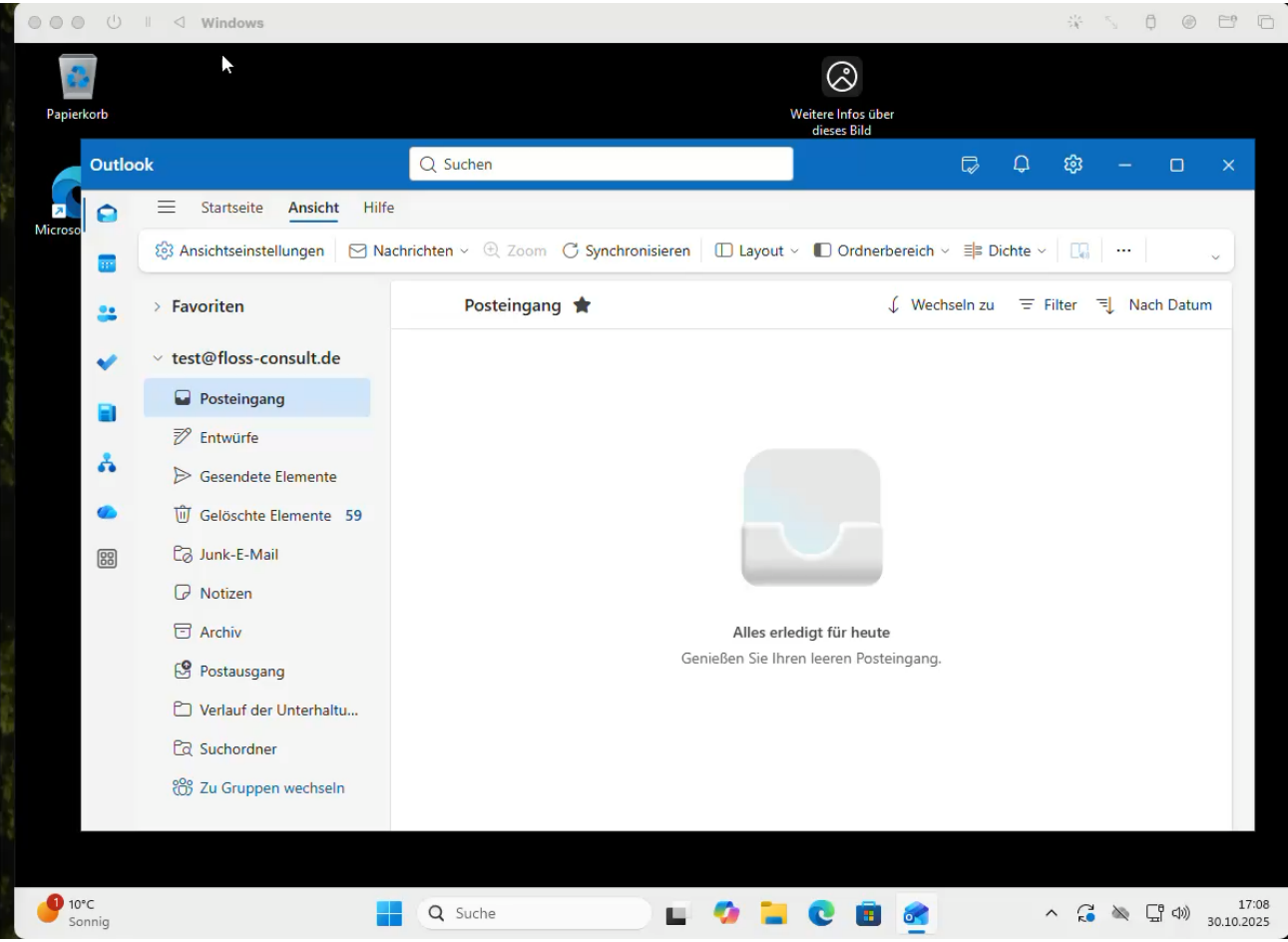


Das Ergebnis

EDV-Unternehmensberatung
Floß GmbH

as-s3c®





EDV-Unternehmensberatung
Floß GmbH

as-s3c®

Was noch wichtig, aber nicht schwer ist

Technische und organisatorische Maßnahmen

EDV-Unternehmensberatung Floß GmbH

as-s3c®

1. Schutzbedarfsanalyse & Risikobetrachtung
2. Datenklassifizierung (öffentlich, intern, vertraulich ...)
3. Technische Maßnahmen wie Berechtigungskonzept, Verschlüsselung
4. Richtlinien (Informationssicherheit, Acceptable Use, …)
5. Datensicherungskonzept

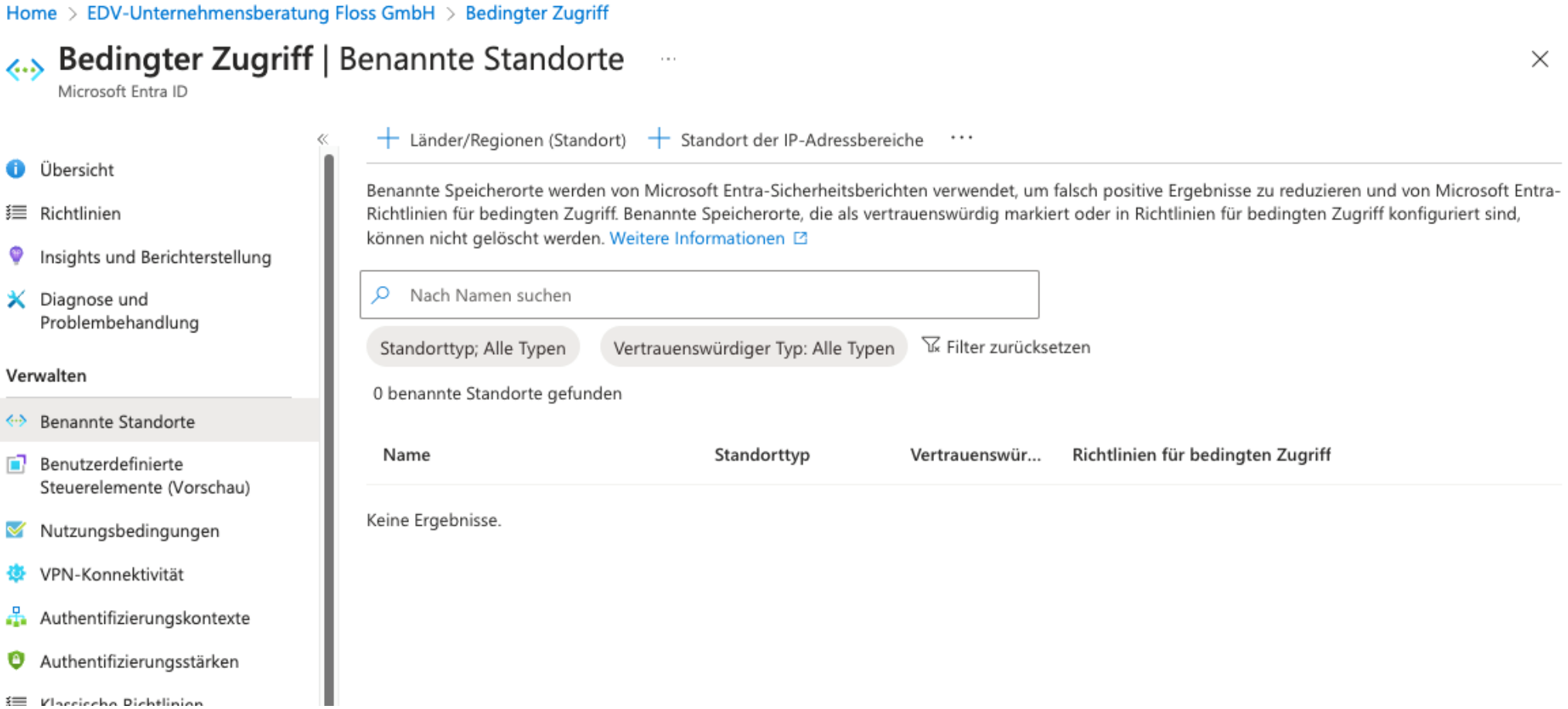
6. Business Continuity (Notfallpläne, Prozessabläufe)
7. Desaster Recovery (je nach Nutzung)
8. Change Prozesse
9. Systemdokumentation
10. Verträge

Technische und organisatorische Maßnahmen

EDV-Unternehmensberatung Floß GmbH

as-s3c®

Ist eine Beschränkung der Regionen/Länder für Zugriffe eingerichtet?



Microsoft 365 Entra Admin Center → Bedingter Zugriff -> Benannte Standorte

Technische und organisatorische Maßnahmen

EDV-Unternehmensberatung Floß GmbH

as-s3c®

Das (Minimum) Berechtigungskonzept:

Bereich / Funktion	Gruppe Admin	Gruppe A	Gruppe B	Gruppe C	Bemerkung / Besonderheit
Bereich I	RWD	R	RW	RWD	Sonderbereich
Bereich II	RWD	RWD	R	R	
.....	RWD	R	R	RWD	

R= Read // W= Write // D= Delete

EDV-Unternehmensberatung
Floß GmbH

as-s3c®