Cloud Assurance

Cloud Assurance umfasst mehr als die Qualität (Quality Assurance) eines Cloud-Dienstes. Immer mehr Unternehmen überlegen, Cloud-Dienste für Geschäftsprozesse in Anspruch zu nehmen. Diese Firmen erwarten von ihren Cloud-Anbietern **Zusicherungen für die Sicherheit und Zuverlässigkeit der Cloud-Dienste.** Das „Information Assurance Framework“ der „European Network and Information Security Agency” (ENISA) definiert einen **Fragenkatalog für Cloud Assurance** (PDF-Download). ENISA empfiehlt Unternehmen, diesen Fragenkatalog von potentiellen Cloud-Anbietern beantworten zu lassen, um eine Einschätzung für die Vertrauenswürdigkeit dieser Anbieter zu erhalten. Der Fragenkatalog ist in zehn Hauptkategorien aufgeteilt.

In den nachfolgenden Abschnitten gibt Fabasoft konkrete Antworten zum Fragenkatalog der ENISA für die Fabasoft Cloud.

Personnel Security

ENISA-Vorgabe:

Hier geht es um Sicherheitsregelungen für das Personal des Cloud-Anbieters. Welche Regelung und Verfahren gibt es, wenn IT-Administratoren oder andere Personen mit Systemzugang angestellt werden? Gibt es Überprüfungen bezüglich Identität, Lebenslauf und Vorstrafen vor der Einstellung? Bietet der Cloud-Anbieter seinem Personal Sicherheitsschulungen an? Gibt es kontinuierliche Überprüfungen und Evaluationen für das Personal?

Fabasoft-Antwort:

Fabasoft sensibilisiert alle Mitarbeiterinnen und Mitarbeiter zum Thema Informationssicherheit. Beim Eintritt in das Unternehmen sind die Vorlage eines Strafregisterauszugs sowie die Unterzeichnung einer Datenschutzerklärung und einer Informationssicherheits-Vereinbarung vorgeschrieben. In der **Fabasoft Academy** finden immer wieder Schulungen zum Thema Informationssicherheit statt. Fabasoft erfüllt darüber hinaus alle Anforderungen für personelle Sicherheit aus der Zertifizierung nach **ISO 27001** und der Prüfung nach **ISAE 3402 Type 2** durch PricewaterhouseCoopers. Dazu gehört insbesondere die **lückenlose Nachvollziehbarkeit und Transparenz** von Aktivitäten in den Cloud-Rechenzentren: jede Aktivität muss vor der Durchführung geplant, angekündigt und im Vier-Augen-Prinzip genehmigt sein. Die Durchführung muss dokumentiert und nachvollziehbar sein.

Supply-Chain Assurance

ENISA-Vorgabe:

Dieses Kriterium hat essentielle Bedeutung, wenn ein Cloud-Anbieter wichtige Operationen an einen Drittanbieter auslagert. Im Wesentlichen betrifft dies vor allem Cloud-Anbieter, die selbst "Infrastructure as a Service"-Leistungen von Drittanbietern für den Betrieb ihrer Cloud-Dienste in Anspruch nehmen, also beispielsweise ihre Cloud-Dienste auf den Plattformen von Amazon oder bei der Deutschen Telekom betreiben. In diesem Fall muss der Cloud-Anbieter darstellen, wie er den Drittanbietern Zugang zur Infrastruktur seiner Cloud-Dienste einräumt und welche Kontrollmechanismen für diese Drittanbieter existieren. Welche Regelungen stellen etwa sicher, dass die Service-Levels, die der Cloud-Anbieter seinen Kunden anbietet, auch von den Drittanbietern eingehalten werden?

Fabasoft-Antwort:

Fabasoft stellt die Cloud-Dienste ausnahmslos mit Fabasoft-eigener Wertschöpfung zur Verfügung. Fabasoft betreibt eigene Cloud-Hardware in Hochleistungsrechenzentren und mietet sich dafür lediglich Raum inklusive Kühlung sowie ausfallsichere Strom- und Internet-Anbindungen. Unsere Rechenzentrums-Partner sind:

Cloud Lokation Deutschland: noris network AG

Cloud Lokation Österreich: T-Systems Austria GesmbH

Cloud Lokation Schweiz: Deltalis SA

Der **vollständige Source-Code** für die Cloud-Dienste **liegt bei Fabasoft**, inklusive der Betriebssysteme und Datenbanksysteme (Enterprise Linux und PostgreSQL).

Betriebssicherheit

ENISA-Vorgabe:

Neben der Garantie von Service-Levels sollte ein Unternehmen sich vergewissern, dass der Cloud-Anbieter angemessene Kontrollen einsetzt, um die unbefugte Offenlegung von Kundendaten zu verhindern. Dies ist in den Bereichen Software Assurance, Patch-Management, Netzwerkarchitekturkontrollen, Host-Architektur, Ressourcenbereitstellung sowie der PaaS- und SaaS-Applikationssicherheit zu hinterfragen.

Software Assurance: Wie schützt der Cloud-Anbieter die Integrität von Betriebssystem und Applikationssoftware? Welche Standards werden dazu eingehalten? Werden Umgebungen bereitgestellt um Risiken zu reduzieren, wie z. B.: Entwicklungs-, Test- und Betriebsumgebungen, und sind diese voneinander getrennt? Welche Kontrollen bieten Schutz gegen schädlichen Code? Wie sehen die Richtlinien und Vorgangsweisen für Backups aus?

Patch-Management: Nach welchem Verfahren erfolgt das Patch-Management? Stellt der Cloud-Anbieter sicher, dass der Patch-Management-Prozess alle Schichten der Cloud-Technologie

abdeckt, wie z. B. Netzwerke, Server-Betriebssysteme, Virtualisierungssoftware, Applikations- und Sicherheitssubsysteme?

Netzwerkarchitektur-Kontrollen: Welche Levels der Isolation werden genutzt (für virtuelle Maschinen, Netzwerke, Speicher, etc.)? Unterstützt die Architektur eine Systemfortsetzung der Cloud, wenn das Unternehmen vom Cloud-Anbieter getrennt wird und auch umgekehrt? Gibt es beispielsweise eine kritische Abhängigkeit zum Benutzerverzeichnis des Kunden?

Host-Architektur: Läuft die Host-Firewall mit den minimal benötigten Ports, um die Services innerhalb der virtuellen Instanz zu unterstützen?

PaaS-Applikationssicherheit: Kann ein "Platform-as-a-Service"-Anbieter die Sicherheit seiner Plattform garantieren? Wie stellt der PaaS-Anbieter sicher, dass auf unternehmensinterne Daten nur das Unternehmenspersonal und Unternehmensapplikationen Zugriff haben? Sorgt der Anbieter dafür, dass die Plattform gegen Verwundbarkeit durch Applikationen geschützt ist?

SaaS-Applikationssicherheit: Beim SaaS-Modell sorgt der Cloud-Anbieter für das Management der Anwendungen. Damit ist der SaaS-Anbieter auch Hauptverantwortlicher für die Sicherheit dieser Applikationen. Welche Administratoren-Kontrollen sind etabliert? Können diese auch genutzt werden, um anderen Benutzern Schreib- und Leserechte zu erteilen? Gibt es detaillierte Zugriffskontrollen und können diese auch an die eigenen Organisationsrichtlinien angepasst werden?

Ressourcenbereitstellung: Wie kann erweitert werden? Garantiert der Anbieter maximal verfügbare Ressourcen in minimaler Zeit? Welche Prozesse werden verfolgt, um Trends im Ressourcenverbrauch zu beherrschen, z. B. saisonale Effekte?

Fabasoft-Antwort:

Fabasoft trennt strikt zwischen Entwicklungs-, Test- und Produktivsystemen. Die Softwareentwicklung erfolgt nach der agilen Projektmanagement-Methodik **SCRUM**. Die Cloud-Dienste werden monatlich mit neuen Cloud-Features aktualisiert. Das Update der Cloud-Dienste erfolgt mit **Zero Known Defects**. Das bedeutet, zum Zeitpunkt des Updates in der Produktivumgebung sind alle bei Fabasoft gemeldeten und erfassten Defekte behoben. Jeder Software-Build durchläuft umfassende **automatische Tests** in einer **Continuous-Integration-Umgebung**, damit potentielle Defekte zu einem möglichst frühen Zeitpunkt erkannt werden. Jeder Cloud-Benutzer kann über den Support-Button in der Cloud-Anwendung direkte Rückmeldungen zu Defekten oder neuen Cloud-Features geben. Diese werden unmittelbar in die agile Softwareentwicklung eingebracht, priorisiert und über die monatlichen Cloud-Updates rasch adressiert **(User Experience Management)**.

Identitäts- und Zugriffsmanagement

ENISA-Vorgabe:

Ein Unternehmen sollte die Identitäts- und Zugriffsmanagementsysteme eines Cloud-Providers hinterfragen: Autorisierung, Identitätsbereitstellung, Management von persönlichen Daten, Key

Management, Encryption, Authentifizierung, Berichtigungsschäden oder Diebstahl, angebotene Identitäts- und Zugriffsmanagementsysteme.

Autorisierung: Gibt es Benutzerkonten, welche systemweite Sonderrechte für die gesamte Cloud haben und wenn ja, welche Rechte sind das (Lese-, Schreibe-, Löschrechte)? Wie werden die Konten mit den höchsten Rechten authentifiziert und gemanagt?

Identitätsbereitstellung: Welche Überprüfungen gibt es bezüglich Identität der Benutzerkonten bei der Registrierung und werden dabei Standards verfolgt?

Management von persönlichen Daten: Sind die Verzeichnisse der Nutzerdaten in einem kompatiblen Format exportierbar? Welche Datenspeicherungs- und Sicherungskontrollen treffen auf die Nutzerverzeichnisse zu?

Verschlüsselung (Encryption): Wo wird Verschlüsselung eingesetzt (Daten im Prozessor, Daten im Speicher, etc.)? Wird Verschlüsselung bei User-Namen und Passwörter eingesetzt? Gibt es eine definierte Richtlinie wofür Verschlüsselung eingesetzt werden muss?

Authentifizierung: Welche Form der Authentifizierung wird für Operationen eingesetzt, welche hohe Assurance benötigen?

Berichtigungsschäden oder Diebstahl: Gibt es eine Erkennung für Diskrepanzen, also die Möglichkeit anormalen oder potentiell schädlichen IP-Verkehr zu detektieren?

Identitäts- und Zugriffsmanagementsysteme: Hier geht es um Identitäts- und Zugriffsmanagementsysteme die vom Cloud-Provider dem Cloud-Kunden zur Nutzung und Kontrolle angeboten werden. Ist der Cloud-Provider kompatibel mit Identitätsprovidern von Dritten? Gibt es die Möglichkeit zum Single-Sign-On? Lässt das System des Client zu, dass Rollen und Verantwortung sowie multiple Domains getrennt werden oder gibt es einen einzigen Key für multiple Domains, Rollen und Verantwortungen? Wie identifiziert der Cloud-Provider sich beim Kunden (z. B.: multiple Authentifizierung)?

Fabasoft-Antwort:

Jede Kommunikation zwischen den Anwendergeräten und den Fabasoft Cloud-Diensten ist ausnahmslos über SSL-Verschlüsselung nach dem RSA-Verfahren geschützt (**HTTPS**-Standard). In den Fabasoft Cloud-Rechenzentren erfolgt die Datenverschlüsselung über **Self Encrpyting Disks**.

Auf Anwendungsebene schützen Fabasoft Cloud-Dienste die Kundendaten vor unberechtigtem Zugriff durch das Konzept der Teamrooms. Ein Teamroom ist ein geschützter Arbeitsbereich in der Cloud, zu dem nur explizit berechtigte (Rechtestufen: Lesen/Bearbeiten/Administration), zur Zusammenarbeit eingeladene und sicher authentifizierte Geschäftskontakte Zugang haben. Pro Teamroom ist eine Sicherheitsstufe festlegbar, die den Zugriff für Personen mit hochwertigen Authentifizierungsmerkmalen beschränkt. Neben der Authentifizierung mit Login-Namen und Passwort unterstützen die Fabasoft Cloud-Dienste **Zwei-Faktor-Authentifizierung** (Mobile-PIN, E-Mail-PIN), Single-Sign-On über Client-Zertifikate (X.509 Standard, auch auf mobilen Devices) und die Anmeldung mit einer **Digitalen Identität** (Österreich: Handysignatur, Deutschland: neuer Personalausweis, Schweiz: SuisseID). Die Authentifizierung erfolgt über ein Fabasoft IDP-Service, das die Standards **SAML** und **OAUTH** implementiert.

Fabasoft unterstützt die Abbildung von Unternehmen mit ihrer Organisationsstruktur in der Cloud (**Cloud-Organisationen**). Zugriffsrechte in Teamrooms sind damit auch für Gruppen und Organisationseinheiten festlegbar, nicht nur für Einzelbenutzer. Das Management der Organisationsmitglieder und die Festlegung von Sicherheitsmerkmalen sind damit auch in der Cloud zentralisierbar.

Asset Management

ENISA-Vorgabe:

Ein Cloud-Anbieter muss eine aktuelle Liste über sein Inventar an Hardware und Software (Applikationen) führen. Dies gibt dem Cloud-Kunden die Sicherheit, dass alle Systeme angemessen kontrolliert werden und es keine Hintertür in die Infrastruktur gibt. Führt der Anbieter eine Liste der Assets, die ein Kunde über eine bestimmte Zeitperiode genutzt hat? Verwendet der Cloud-Provider eine automationsgestützte Inventarisierung?

Fabasoft-Antwort:

Fabasoft ist zertifiziert nach dem **Standard ISO 20000** und erfüllt damit alle Anforderungen dieses Standards für die automationsgestützte Führung des Hardware- und Software-Inventars.

Data and Services Portability

ENISA-Vorgabe:

Unternehmen müssen das Lock-in-Risiko bei einem Cloud-Anbieter hinterfragen. Gibt es dokumentierte Prozeduren oder APIs für den Datenexport aus der Cloud? Stellt der Lieferant kompatible Formate für den Export von Daten zur Verfügung? Sind APIs standardisiert?

Fabasoft-Antwort:

Die Fabasoft Cloud-Dienste unterstützen die Standards **CMIS (Content Management Interoperability Standard), WebDAV** und **CalDAV** für den Import und den Export von Cloud-Daten. Damit ist es beispielsweise möglich, einen Fabasoft Cloud-Dienst als **Netzwerklaufwerk** unter Microsoft Windows oder im Apple Finder einzurichten und über Backup-Werkzeuge einen kontinuierlichen Delta-Datenabgleich aus der Cloud oder in die Cloud durchzuführen. Auch der Import und Export von Daten im **XML-Format** steht zur Verfügung.

Business Continuity Management

ENISA-Vorgabe:

Ein Cloud-Anbieter muss seinen Kunden die Kontinuität des Cloud-Betriebs im Schadensfall glaubhaft darstellen. Hat der Provider dokumentiert welche Auswirkungen ein Schadenfall hätte? Was wäre dabei der Wiederherstellungszeitpunkt und was die Wiederherstellungsdauer? Welche Abhängigkeiten zu Lieferanten und Outsourcing-Partnern existieren für den Wiederherstellungsprozess? Können die Auswirkungen eines störenden Ereignisses auf einem akzeptablen Niveau gehalten werden (Unfallmanagement)? Gibt es beim Provider einen formalen Prozess, welcher Vorfälle herausfindet, identifiziert, analysiert und adressiert? Wird dieser Prozess geprobt und vorbereitet, sodass bei einem richtigen Vorfall dieser effektiv bewältigt werden kann? Wie werden Vorfälle dokumentiert und Beweise gesichert?

Fabasoft-Antwort:

Fabasoft erfüllt die Anforderungen für die Kontinuität des Cloud-Betriebs im Schadensfall nach den Anforderungen aus der Zertifizierung nach **ISO 20000** und aus der Prüfung nach **ISAE 3402 Type 2** durch PricewaterhouseCoopers.

Physical Security

ENISA-Vorgabe:

Die physische Sicherheit ist deshalb so wichtig, weil viele Cloud-Anbieter die Kontrolle über ihre IT-Infrastruktur an einen Dritten weitergeben, also outsourcen. Welche Assurance können Cloud-Anbieter dem Kunden geben bezüglich der physischen Sicherheit des Standortes? Wer hat zum Beispiel neben dem IT-Personal noch Zugriff auf die IT-Infrastruktur (z. B.: Reinigungspersonal)? Wie oft werden Zugriffsrechte erneuert? Wird das Personal, das auf sicherere Bereiche Zugriff hat, überwacht? Verwendet das Personal portables Equipment, wie Laptops oder Smartphones, welche Zugriff auf das Rechenzentrum ermöglicht?

Fabasoft-Antwort:

Alle Fabasoft Cloud-Rechenzentren sind mit Alarmsystemen ausgestattet, die im Falle eines nicht erlaubten Zutrittsversuches sofort die Exekutive verständigen. Zusätzlich sind die Rechenzentren mit Videoüberwachung ausgestattet. Der Zutritt zu den Rechenzentren ist nur wenigen autorisierten Mitarbeitern gestattet.

Umweltbedingte Sicherheitsregelungen

ENISA-Vorgabe:

Welche Prozeduren oder Regelungen gibt es, welche dafür sorgen, dass Umweltangelegenheiten keine Unterbrechungen des Services fordern? Welche Methoden werden genutzt um sich vor Schäden wie Feuer, Flut oder Erdbeben zu schützen?

Fabasoft-Antwort:

Der Betrieb der Fabasoft Cloud-Dienste erfolgt in insgesamt **drei Rechenzentren pro Cloud-Lokation**. Die beiden aktiven Rechenzentren (Rechenzentrum 1 und Rechenzentrum 2) befinden sich an zwei unterschiedlichen Standorten. Das Backup-Rechenzentrum befindet sich am Standort des Rechenzentrums 1. Die beiden Standorte der aktiven Rechenzentren pro Fabasoft Cloud-Lokation sind **mindestens 2 km** voneinander entfernt. Beide Rechenzentren sind jeweils mit redundanter Klimatisierung und redundanter Netzwerkinfrastruktur ausgestattet. Im Falle einer Unterbrechung der Stromversorgung können alle Rechenzentren die Stromversorgung der Komponenten für bis zu 15 Minuten aufrechterhalten. Mindestens ein Rechenzentrum pro Cloud-Lokation kann die Stromversorgung der eingesetzten Komponenten über eine **USV mit angeschlossenem Diesel-Notstromaggregat** auch bei längerer Unterbrechung aufrechterhalten.

Im Backup-Rechenzentrum wird eine Backup-Infrastruktur zur Sicherung aller Daten betrieben. Das Backup-Rechenzentrum ist mit eigener Zutrittsregelung, redundanter Klimatisierung und Netzwerkinfrastruktur sowie einer Notstromversorgung ausgestattet.

Die Rechenzentren sind mit Brandfrühesterkennung bzw. präventivem Brandschutz ausgestattet.

Legal Requirements

ENISA-Vorgabe:

Unternehmen haben Compliance-Verpflichtungen und müssen sicherstellen, dass sie diese Verpflichtungen auch bei Nutzung von Cloud-Diensten einhalten. In welchem Land hat der Cloud-Provider seinen Standort? Ist die Cloud-Infrastruktur des Providers im selben Land, oder in einem anderen? Wo werden die Cloud-Daten physisch abgespeichert? Was passiert mit den Daten die zum Cloud-Provider gesendet werden nach dem Ablauf des Vertrags?

Fabasoft-Antwort:

Die Fabasoft Cloud-Rechenzentren liegen in Deutschland, in Österreich und in der Schweiz und **unterliegen damit dem EU-Recht**. Mit dem einzigartigen Konzept der Cloud-Lokationen bietet Fabasoft seinen Kunden die Wahlfreiheit und die Gewissheit, wo die Speicherung der Cloud-Daten erfolgt. So haben Sie stets Kenntnis über den Datenstandort.