RELion ONE in der Microsoft Cloud

Service Level Agreement

Deutschland und Österreich

Inhalt

1 Einleitung

Dieses Service Level Agreement (SLA) gilt für RELion ONE bei Betrieb in der Microsoft „public" Cloud (New Commerce Experience-Modell (NCE). RELion ist als immobilienwirtschaftliche Branchenlösung eine Ergänzung („Extension") zum online-Service Dynamics 365 Business Central von Microsoft. Ein Anwender kann RELion ONE von jedem internetfähigen Endgerät mit modernem Browser nutzen. Ein direkter Zugriff durch den Anwender auf die physische Infrastruktur, den SQL-Server oder lokale Ressourcen des Rechenzentrums sind nicht möglich. Zur Kommunikation mit der Anwendung stehen grundsätzlich Webservices (APIs) zur Verfügung, über die die Integration in die Umfeldsysteme und Services des Kunden erfolgen kann. Dazu kann ein Kunde eigene Entwicklung erstellen oder von Dritten erstellen lassen und diese ebenfalls als Extension in die Umgebungen einbinden. Alle Extensions müssen Cloud-ready erstellt werden und die Voraussetzungen von Microsoft erfüllen. Diese Extension wird im Rahmen dieses SLA von der Auftragnehmerin (Aareon) weder betreut noch gepflegt.

Im Rahmen des Cloud-Services werden keine Daten, wie z.B. Indexreihen, Mietenspiegel, Steuersätze oder andere Einrichtungen bereitgestellt. Die Datenpflege wird vom Kunden erbracht.

Alle Leistungen in Zusammenhang mit dem Betrieb und der Azure-Umgebung werden in einer Vereinbarung geregelt, die zwischen Microsoft und dem Endkunden direkt zu Stande kommt (Microsoft Customer Agreement). Der technische Betrieb erfolgt durch Microsoft in dessen Azure-Umgebung. Microsoft stellt damit die physikalische Ausstattung des Rechenzentrums einschließlich der notwendigen Systemsoftware zur Verfügung. Darum folgt zunächst die Erläuterung der Microsoft-Services für Dynamics 365 Business Central.

Quelle: https://learn.microsoft.com/en-us/dynamics365/business-central/dev-itpro/service-overview.

2 Microsoft Dynamics 365 Business Central

RELion ONE nutzt die Plattform Microsoft Dynamics Business Central. Eine Plattform, die verschiedene Zertifizierungen erfüllt, darunter ISO27001/SOC 1 und 2 (vgl. ISAE 3402). Produktionsinstanzen sind nach den Business Continuity-Standards von Microsoft eingerichtet und verfügen über eine hohe Verfügbarkeit und sind mit Disaster Recovery ausgestattet.

2.1 Einschränkungen

Diese SLA und alle zutreffenden Servicelevels gelten nicht für folgende Leistungs- oder Verfügbarkeitsprobleme:

1. aufgrund von Faktoren, die außerhalb unserer Kontrolle liegen (z. B. Naturkatastrophen, Kriege, Terroranschläge, Aufstände, staatliche Maßnahmen, Netz- oder Geräteausfall außerhalb unserer Rechenzentren, u.a. an Ihrem Standort oder zwischen Ihrem Standort und unserem Rechenzentrum),
2. die aus der Nutzung von Diensten, Hardware oder Software hervorgehen, die nicht von Microsoft bereitgestellt wurden, darunter u. a. Probleme im Zusammenhang mit unzureichender Bandbreite oder Software bzw. Diensten von Dritten,
3. Dies ist die Folge von Ausfällen an einem einzelnen Microsoft Datacenter-Standort, wenn die Netzwerkverbindung des Kunden explizit von diesem Standort in nicht geostabiler Weise abhängig ist.
4. die durch die Nutzung eines Diensts verursacht wurden, nachdem Microsoft den Kunden angewiesen hat, die Nutzung des Dienstes zu ändern, und der Kunde seine Nutzung nicht wie angewiesen geändert hat,
5. während oder bezüglich einer Vorschau, Vorabversion, Beta- oder Testversion eines Diensts, eines Features oder von Software (wie von uns bestimmt) oder Käufen, die mit Abonnementgutschriften von Microsoft getätigt wurden,
6. die durch nicht autorisierte Handlung oder Unterlassung des Kunden einer erforderlichen Handlung oder die Kundenmitarbeiter oder -vertreter, Vertragspartner oder Lieferanten oder durch andere Personen verursacht wurden, die sich mithilfe der Kennwörter oder Geräte des Kunden Zugriff auf das Microsoft-Netzwerk verschafft haben, oder die auf andere Weise von der Nichtbefolgung angemessener Sicherheitsverfahren durch die Kunden verursacht werden,
7. die durch das Versäumnis des Kunden, erforderliche Konfigurationen einzuhalten, unterstützte Plattformen zu verwenden, Richtlinien für die akzeptable Nutzung einzuhalten, aufgrund der Kundennutzung des Diensts, die nicht mit den Features und Funktionen des Dienstes vereinbar ist (z. B. Versuche, nicht unterstützte Vorgänge durchzuführen) oder die nicht den von Microsoft veröffentlichten Hilfestellungen entspricht, verursacht wurden,
8. die sich aus fehlerhaften Eingaben, Anweisungen oder Argumenten ergeben (z. B. Anforderung von Zugriff auf nicht vorhandene Dateien),

9. die sich aus Kundenversuchen ergaben, Vorgänge durchzuführen, die vorgeschriebene Kontingente überschreiten oder die sich aus der Drosselung von angenommenem missbräuchlichem Verhalten durch Microsoft ergeben,
10. aufgrund der Kundennutzung der Dienstfunktionen, die außerhalb des zugeordneten Unterstützungszeitraums liegen, oder
11. für zum Zeitpunkt des Vorfalls reservierte, aber nicht bezahlte Lizenzen.
12. die durch den Kunden eingeleiteten Vorgänge wie Neustart, Stopp, Start, Failover und Skalierung von Rechenleistung und Speicher, die Ausfallzeiten verursachen, werden von der Betriebszeitberechnung ausgeschlossen.
13. monatliche Wartungsfenster, die eine Ausfallzeit zum Patchen des Kundenservers und Infrastruktur verursachen, werden von der Betriebszeitberechnung ausgeschlossen.

2.2 Geschäftskontinuität und Notfallwiederherstellung (BCDR)

Die Online-Architektur und die Verwaltungsfunktionen von Business Central gewährleisten einen unterbrechungsfreien Zugriff auf Ihre kritischen Geschäftsdaten und -prozesse. Automatische Backups, integrierte Redundanz und Hochverfügbarkeit schützen Ihre Daten und sorgen dafür, dass sie während und nach einem störenden Ereignis zugänglich bleiben. Business Central verfügt über proaktive BCDR-Strategien, -Prozesse und -Technologien, die Ausfallzeiten minimieren und wichtige Ressourcen erhalten.

Business Central nutzt die Azure-Cloud-Computing-Plattform für ihre robusten Business-Continuity-Optionen, die Ihre kritischen Workloads vor Unterbrechungen schützen. Das globale Regionsnetzwerk von Azure sorgt dafür, dass sich Ihre Daten in der Nähe Ihres geografischen Standorts befinden, und bietet Optionen zum Wiederherstellen von Daten in einer anderen Region. Ihre Daten sind trotz regionaler Ausfälle oder Störungen verfügbar. Weitere Informationen zu Azure-Regionen finden Sie unter https://azure.microsoft.com/de-de/explore/global-infrastructure/geographies/#overview.

Administratoren können das Business Central Admin Center verwenden, um die Azure-Region zu finden, in der sich ihre Umgebungen befinden.

2.3 Datenbank und Backups

Business Central verwendet Azure SQL-Datenbank als Datenbanktechnologie für seine Umgebungen. Azure SQL-Datenbank ist ein vollständig verwalteter relationaler Datenbankdienst mit integrierter Hochverfügbarkeit, Sicherungen sowie lokaler und regionaler Redundanz. Weitere Informationen dazu, wie Azure SQL-Datenbank für eine reibungslose Ausführung von Workloads sorgt, finden Sie unter https://learn.microsoft.com/en-us/azure/azure-sql/database/high-availability-sla?view=azuresql.

Azure SQL-Datenbank schützt Business Central-Produktions- und Sandboxumgebungen, indem automatische Sicherungen erstellt werden, die 28 Tage lang aufbewahrt werden. Administratoren können das Business Central Admin Center verwenden, um die Umgebung zu einem bestimmten Zeitpunkt in den letzten 28 Tagen wiederherzustellen. Weitere Informationen zum Wiederherstellen einer Umgebung finden Sie unter https://learn.microsoft.com/en-us/dynamics365/business-central/dev-itpro/administration/tenant-admin-center-backup-restore.

Administratoren können auch das Business Central Admin Center verwenden, um gelöschte Produktions- oder Sandbox-Umgebungen innerhalb von sieben Tagen nach ihrer Löschung wiederherzustellen. Weitere Informationen zum Wiederherstellen gelöschter Umgebungen finden Sie unter Wiederherstellen einer Umgebung (https://learn.microsoft.com/en-us/dynamics365/business-central/dev-itpro/administration/tenant-admin-center-environments-delete#recover-an-environment).

2.4 Produktiv- und Testumgebungen

2.4.1 Produktivumgebungen

Produktivumgebungen sollen genau das sein: Umgebungen, in denen ein Unternehmen sein Tagesgeschäft in Business Central ausführen kann, die auf Leistungsstufen in Azure mit einem garantiert hohen Maß an Verfügbarkeit und Support bereitgestellt werden.

Produktionsumgebungen werden automatisch und häufig gesichert, um Geschäftsdaten zu schützen. Weitere Informationen finden Sie unter https://learn.microsoft.com/en-us/dynamics365/business-central/dev-itpro/faq#how-often-are-production-databases-backed-up.

Sie können zusätzliche Produktivumgebungen erstellen, z. B. für Schulungen oder Leistungstests. Zu Schulungszwecken ziehen es Unternehmen jedoch in vielen Fällen vor, eine Sandbox-Umgebung mit Produktionsdaten zu erstellen. Sie können auch zusätzliche Produktionsumgebungen erstellen, um Niederlassungen in verschiedenen Ländern/Regionen zu unterstützen.

Anmerkung

Mit den Abonnementtypen Premium und Essential erhält jeder Business Central-Kunde eine Produktionsumgebung und drei Sandbox-Umgebungen ohne Aufpreis. Wenn der Kunde mehr Produktionsumgebungen benötigt, kann er über die Auftragnehmerin als CSP-Partner des Kunden zusätzliche Umgebungen erwerben. Jede zusätzliche Produktionsumgebung verfügt über drei zusätzliche Sandbox-Umgebungen und 4 GB zusätzliche, mandantenweite Datenbankkapazität. Darüber hinaus gibt es ab dem 2. Veröffentlichungszyklus 2023 ein Limit für die Anzahl der Unternehmen, die Sie auf einem einzelnen Mandanten haben können (siehe https://learn.microsoft.com/en-us/dynamics365/business-central/dev-itpro/administration/operational-limits-online#company-limit-per-environment).

Administratoren können die zusätzlichen Umgebungen in der Business Central-Verwaltungskonsole erstellen. Die Umgebungen können in jedem Land oder jeder Region erstellt und verwendet werden, in dem Business Central verfügbar ist, einschließlich der Länder oder Regionen, in denen die vorhandenen Umgebungen des Kunden ausgeführt werden. Das Umgebungskontingent wird angewendet, wenn Sie versuchen, eine neue Umgebung zu erstellen oder eine vorhandene Umgebung in der Business Central-Verwaltungskonsole zu kopieren.

Anmerkung

Eine Produktivumgebung kann den Status "Angehalten" aufweisen, wenn das Abonnement angehalten wurde oder wenn über einen längeren Zeitraum nicht auf die Umgebung zugegriffen wurde. In diesen Fällen können Sie Erweiterungen nur dann in einer solchen

Umgebung veröffentlichen, wenn sie nur über Evaluierungsunternehmen verfügt. Wenn die angehaltene Umgebung für die tatsächliche Produktion verwendet wurde, sodass sie Unternehmen enthält, die keine Evaluierungsunternehmen sind, können Sie keine Erweiterungen veröffentlichen.

2.4.2 Verwalten von Produktivumgebungen

Der Kunde kann die Business Central-Verwaltungszentrale nutzen, um die Umgebungen manuell zu verwalten. Weitere Informationen sind unter dem folgenden Link erreichbar: https://learn.microsoft.com/en-us/dynamics365/business-central/dev-itpro/administration/tenant-admin-center-environments.

2.4.3 Sandbox-Umgebungen

Sandbox-Umgebungen sollen genau das sein: Umgebungen, mit denen Sie herumspielen, die Sie als Testumgebung für die Entwicklung verwenden und nach Belieben löschen können. Sie können Apps direkt aus Visual Studio Code in einer Sandkastenumgebung bereitstellen und eine Debugsitzung an eine Sandbox anfügen.

Wichtig

Apps, die aus der Entwicklungsumgebung in einer Sandbox veröffentlicht oder mit Designer erstellt (https://learn.microsoft.com/en-us/dynamics365/business-central/dev-itpro/developer/devenv-inclient-designer) wurden, werden im Bereich des Dienstknotens veröffentlicht, der die Umgebung hostet. Wenn die Sandbox aktualisiert wird, werden diese Apps entfernt, da die Umgebung auf einen anderen Knoten verschoben wird, auf dem die neue Version ausgeführt wird. Die Daten der App werden jedoch nicht entfernt, sodass Sie die App nur erneut veröffentlichen und installieren müssen, um sie verfügbar zu machen.

Apps, die mithilfe der Aktion "Erweiterung hochladen" auf der Seite "Erweiterungsverwaltung" in die Umgebungen beider Typen (Produktion und Sandbox) hochgeladen werden, werden in einem globalen Bereich veröffentlicht. Wenn die Umgebung aktualisiert oder verschoben wird, werden diese Apps auf den Dienstknoten heruntergeladen und installiert, was bedeutet, dass sie nicht verschwinden.

Sie können Sandkästen auch sicher für das Training verwenden, z. B. zum Befolgen eines Lernpfads von Microsoft Learn (https://learn.microsoft.com/en-us/training/dynamics365/business-central?WT.mc_id=dyn365bc_landingpage-docs), da es sich um eine sichere Umgebung zum Experimentieren handelt. Wenn etwas schief geht, löschen Sie einfach die Sandbox und beginnen von vorne.

Wichtig

Die automatische Sicherung, die für Produktionsumgebungen gilt, gilt nicht für Sandbox-Umgebungen. Wenn Sie Daten aus einer Sandbox-Umgebung exportieren möchten, können Sie Excel oder RapidStart verwenden, aber Sie können keinen Datenbankexport anfordern.

Sie können eine Sandbox-Umgebung erstellen, die Daten aus Ihrer Produktionsumgebung enthält, z. B. zu Debugging-Zwecken. Wenn Sie jedoch Leistungstests oder ähnliche

Benchmarks durchführen möchten, ist die Sandbox für diesen Zweck nicht zuverlässig genug. Dies liegt daran, dass Sandkästen in Azure in einer anderen Leistungsstufe ausgeführt werden als Produktionsumgebungen. Erstellen Sie stattdessen eine dedizierte Umgebung, die auf dem Produktionsumgebungstyp basiert, um genau die Erfahrung und Leistung zu erhalten, die Benutzer in der tatsächlichen Produktionsumgebung erleben werden. Weitere Informationen finden Sie unter https://learn.microsoft.com/en-us/dynamics365/business-central/dev-itpro/performance/performance-online.

Sandkastenumgebungen sind für bestimmte Arten von Entwicklungsszenarien praktisch, da der Debugendpunkt standardmäßig geöffnet ist. Dies bedeutet, dass Sie Visual Studio Code an ein ausgeführtes System anfügen und über ausgeführten Code debuggen können. Außerdem können Sie damit direkt aus Code in der Umgebung veröffentlichen.

Wichtig

Ausgehende HTTP-Aufrufe von Apps/Erweiterungen werden standardmäßig blockiert und müssen für jede Nebenstelle genehmigt werden, andernfalls zeigt das System anstelle eines externen Aufrufs die folgende Fehlermeldung an: Die Anforderung wurde von der Laufzeit blockiert, um eine versehentliche Verwendung von Produktionsdiensten zu verhindern.

Um ausgehende HTTP-Aufrufe zu aktivieren, gehen Sie zur Seite Erweiterungsverwaltung in Business Central und wählen Sie Konfigurieren aus. Stellen Sie dann auf der Seite Erweiterungseinstellungen sicher, dass HttpClient-Anforderungen zulassen ausgewählt ist. Diese Einstellung muss für jede App/Erweiterung aktiviert werden, einschließlich Bibliotheks-Apps.

Wenn Ihre Organisation über mehr als eine Sandbox-Umgebung verfügt, können Sie zwischen Umgebungen wechseln, indem Sie den App Launcher öffnen, die Kachel Dynamics 365 und dann die Kachel Business Central Sandbox auswählen. Die Auswahl der Sandbox-Umgebung zeigt die verfügbaren Sandboxen an, also wählen Sie diejenige aus, zu der Sie wechseln möchten. (https://learn.microsoft.com/en-us/dynamics365/business-central/dev-itpro/administration/environment-types)

2.5 Hochverfügbarkeit durch geografische Redundanz

Jede Business Central-Umgebung ist außerdem durch automatische georedundante Backups geschützt. Wenn es in einer Region zu einem vollständigen Ausfall kommt, stellt Azure Ihre Daten aus der Sicherung in einer anderen Azure-Region innerhalb derselben Azure-Geografie wieder her. Obwohl es selten vorkommt, ist die Wiederherstellung von Daten in einer anderen Azure-Region ein vollständig automatisiertes internes Verfahren, das wir regelmäßig praktizieren. Es ist ein Standardbestandteil interner Audits und Disaster-Recovery-Übungen. Weitere Informationen zu Sicherungen finden Sie unter https://learn.microsoft.com/en-us/azure/azure-sql/database/automated-backups-overview?view=azuresql).

Azure-Verfügbarkeitszonen bieten zusätzliche Resilienz (https://learn.microsoft.com/en-us/azure/reliability/availability-zones-overview?tabs=azure-cli), indem sie physisch getrennte Rechenzentren innerhalb einer Azure-Region bieten. Durch die Verteilung von Ressourcen auf mehrere Verfügbarkeitszonen wird eine hohe Verfügbarkeit für die Rechen- und Speicherressourcen für Business Central erreicht. Bei lokalen Ausfällen oder geplanten

Wartungsarbeiten in einer oder mehreren Zonen sind Mandanten in den verfügbaren Zonen nicht betroffen. Andere Mandanten werden automatisch an Ressourcen in den verfügbaren Zonen in derselben Region umgeleitet. Diese Option ist für alle Business Central-Produktionsumgebungen mit kostenpflichtigen Business Central-Abonnements aktiviert.

Business Central ist außerdem mit integrierten Redundanz-, Auto-Scaling- und automatischen Lastenausgleichsfunktionen für seine Computing-Ressourcen ausgestattet. Um verfügbar zu bleiben, wenn eine oder mehrere seiner Compute-Instanzen ausfallen, wird Business Central auf anderen Instanzen ausgeführt. Business Central unterstützt fortlaufende Upgrades und automatisierte Betriebssystem-Image-Updates, um Patches, Sicherheitsupdates oder neue Plattformversionen ohne Ausfallzeiten anzuwenden. Compute-Instanzen sind immer auf dem neuesten Stand und sicher, was die Anfälligkeit für Bedrohungen und Dienstunterbrechungen verringert.

2.6 Vereinbarungen zum Servicelevel (SLA)

Business Central Online unterliegt der Modern Lifecycle-Richtlinie (https://learn.microsoft.com/de-DE/lifecycle/policies/modern). Die Bedingungen für Vereinbarungen zum Servicelevel werden in dem Dokument beschrieben, das Sie auf der **Seite Lizenzbedingungen im** Abschnitt Vereinbarungen zum Servicelevel für Microsoft Online Services (https://www.microsoft.com/licensing/docs/view/licensing-use-rights?rtc=1icensing Documents (microsoft.com)herunterladen können.

Darüber hinaus können Administratoren die Integrität eines Mandanten überwachen und Upgradefenster in der Business Central-Verwaltungskonsole angeben (https://learn.microsoft.com/en-us/dynamics365/business-central/dev-itpro/administration/tenant-admin-center).

Datenbanken werden durch automatische Backups geschützt, die 28 Tage lang aufbewahrt werden. Die Sicherung enthält Daten aus allen Produktions- und Sandbox-Umgebungen, die in der Datenbank enthalten sind. Administratoren eines Business Central-Mandanten können nicht direkt auf diese Sicherungen zugreifen oder diese verwalten, da sie automatisch von Microsoft verwaltet werden. Administratoren können ihre Umgebungen jedoch mithilfe des Business Central Admin Centers zu einem bestimmten Zeitpunkt in der Vergangenheit wiederherstellen. Weitere Informationen finden Sie unter https://learn.microsoft.com/en-us/dynamics365/business-central/dev-itpro/administration/tenant-admin-center-backup-restore und https://learn.microsoft.com/en-us/azure/azure-sql/database/automated-backups-overview?view=azuresql.

Weitere Informationen zu Azure SQL finden Sie unter https://learn.microsoft.com/en-us/azure/azure-sql/database/high-availability-sla?view=azuresql&tabs=azure-powershell.

2.7 Service-Updates

Business Central Online ist ein Dienst, der aus einer von Microsoft verwalteten Plattform und Geschäftsfunktionen besteht. Viele Microsoft-Partner bieten zusätzliche Geschäftsfunktionen an, z.B. für bestimmte Branchen- oder Lokalisierungsanforderungen. Sowohl die Geschäftsfunktionalität als auch die Servicekomponenten werden von Microsoft kontinuierlich überwacht und bei Bedarf aktualisiert.

Neue Funktionen werden in Veröffentlichungswellen durch Microsoft eingeführt, die aus einem Hauptupdate und monatlichen Nebenupdates bestehen. Die meisten Funktionen werden in Hauptupdates zur Verfügung gestellt, aber einige werden in kleineren Updates verfügbar. Kritische Fixes werden so schnell wie möglich ausgerollt, nachdem sie Tests bestanden haben und in der geschützten Stagingumgebung von Microsoft überprüft wurden. Sie können sich jederzeit den Versionsplan einsehen, https://learn.microsoft.com/en-us/dynamics365/release-plans/um einen Überblick über neue und bevorstehende Funktionen zu erhalten. Kleinere Updates finden Sie unter https://learn.microsoft.com/en-us/dynamics365/business-central/dev-itpro/whatsnew/whatsnew-update-23-5.

Administratoren können ein Wartungsfenster festlegen, in dem Microsoft jede Umgebung aktualisieren kann. Weitere Informationen finden Sie unter https://learn.microsoft.com/en-us/dynamics365/business-central/dev-itpro/administration/tenant-admin-center-update-management. Microsoft plant dann Updates der Geschäftsfunktionen, die während dieser Wartungsfenster angewendet werden sollen.

Eine Ausnahme von dieser Art von Zeitplan sind die kontinuierlichen Aktualisierungen des zugrunde liegenden Dienstes. Die Dienstkomponenten gelten für mehrere Umgebungen, z. B. für alle Mandanten in einer Region. Daher plant Microsoft diese Updates für eine Zeit, in der der Datenverkehr in den einzelnen Regionen geringer ist, in der Regel abends oder nachts. In der Regel bemerken Benutzer Dienstaktualisierungen nicht. Business Central verwaltet den Datenverkehr, sodass Personen, die in Business Central arbeiten, nicht betroffen sind.

2.8 Service-Betrieb

Business Central wird weltweit in vielen Microsoft Azure-Rechenzentren ausgeführt. Alle Teile der Infrastruktur und der Dienste werden kontinuierlich überwacht und optimiert, um das bestmögliche Erlebnis zu bieten. Die meisten Servicevorgänge und -optimierungen finden statt, ohne dass sich die Benutzer dessen bewusst sind. In einigen Situationen ist eine Benutzerinteraktion erforderlich, z. B. eine erneute Verbindung mit Business Central herzustellen oder den Browser zu aktualisieren. Der Benutzer wird direkt im Browser benachrichtigt, wenn eine Aktion seinerseits erforderlich ist. Benutzer werden aufgefordert, Maßnahmen zu ergreifen, bevor die Optimierungen auf den Dienst angewendet werden. So können sie ohne weitere Unterbrechungen weiterarbeiten. Der Servicebetrieb findet prinzipiell an jedem Tag und über den ganzen Tag statt.

2.9 Zuverlässigkeit

Microsoft stellt regelmäßig Funktionsupdates für den zugrunde liegenden Dienst und gezielte bedarfsgesteuerte Korrekturen bereit, um Probleme mit der Dienstqualität zu beheben. Der Freigabeprozess umfasst eine umfassende Reihe von Quality Gates:

- Gründliche Code-Reviews
- Ad-hoc-Tests
- Automatisierte komponenten- und szenariobasierte Tests
- Feature-Management
- Regionaler sicherer Einsatz

Doch selbst mit diesen Sicherheitsvorkehrungen kann es zu Vorfällen kommen. Live-Site-Vorfälle können in mehrere Kategorien unterteilt werden:

- Probleme mit abhängigen Diensten, z. B. Microsoft Entra ID, Azure SQL, Speicher, VM-Skalierungsgruppe, Service Fabric usw.
- Infrastrukturausfall, z. B. Hardware- oder Rechenzentrumsausfall
- Konfigurationsprobleme für Business Central-Umgebungen, z. B. unzureichende Kapazität
- Code-Regressionen in Business Central online
- Kundenspezifische Fehlkonfigurationen, wie z. B. fehlerhafte Abfragen oder Berichte, oder andere Arten von problematischem AL-Code.

Die Reduzierung des Vorfallvolumens ist eine Möglichkeit, die Belastung der Live-Site zu verringern und die Kundenzufriedenheit zu verbessern. Dies ist jedoch nicht immer möglich. Zum Beispiel, wenn Vorfallkategorien außerhalb der direkten Kontrolle des Business Central-Teams liegen. Wenn der Service-Footprint erweitert wird, um ein schnelles Wachstum der Nutzung zu unterstützen, steigt auch die Wahrscheinlichkeit, dass ein Vorfall aufgrund externer Faktoren auftritt. Es kann zu einer hohen Anzahl von Vorfällen kommen, selbst in Fällen, in denen der Business Central-Dienst minimale Servicecode-Regressionen aufweist und wenn der Service sein Service Level Objective (SLO) für eine Gesamtzuverlässigkeit von 99,95 % erreicht oder übertroffen hat. Das Business Central-Team wendet erhebliche Ressourcen auf, um die Kosten für Vorfälle auf ein nachhaltiges Niveau zu senken, sowohl durch finanzielle als auch durch technische Maßnahmen.

Ausfallzeit: Zeiträume, in denen sich Endbenutzer nicht in ihre Instanz einloggen können.

Betriebszeitprozentsatz: Der Betriebszeitprozentsatz errechnet sich nach folgender Formel:

$$\frac{Nutzerminuten\ abzüglich\ Ausfallzeit}{Nutzerminuten}\ x\ 100$$

wobei die Ausfallzeit in Nutzerminuten gemessen wird, d. h. für jeden anwendbaren Zeitraum ist die Ausfallzeit die Summe der Dauer (in Minuten) jedes Vorfalls, der während dieses Anwendbaren Zeitraums auftritt, multipliziert mit der Anzahl der von diesem Vorfall betroffenen Nutzer.

Servicegutschrift:

Betriebszeitprozentsatz	Servicegutschrift
< 99,9 %	25 %
< 99 %	50 %
< 95 %	100 %

2.10 Live-Site-Incident-Management

Bei der Untersuchung von Live-Site-Vorfällen folgt das Business Central-Team einem Standardbetriebsprozess, der bei Microsoft und in der Branche üblich ist.

Die wichtigsten Schritte im Lebenszyklus des standardmäßigen Live-Site-Incident-Managements werden nachfolgend erläutert.

In der ersten Phase, der **Serviceüberwachungsphase,** arbeitet das Entwicklungs- und Betriebsteam (DevOps) mit Ingenieuren, Programmmanagern und dem Senior Leadership Team zusammen, um Service Level Indicators (SLIs) und Service Level Objectives (SLOs) sowohl für Haupt- als auch für Nebenszenarien zu definieren. Diese Ziele gelten für verschiedene Metriken des Diensts, einschließlich der Zuverlässigkeit von Szenarien/Komponenten, der Leistung von Szenarien/Komponenten (Latenz) und des Ressourcenverbrauchs. Das Live-Site-Team und das Produktteam erstellen dann Warnungen, die Service Level Indicators (SLIs) im Vergleich zu vereinbarten Zielen überwachen. Wenn Verstöße festgestellt werden, wird eine Warnung zur Untersuchung ausgelöst.

In der zweiten Phase, der **Incident-Response-Phase, werden** die Prozesse so strukturiert, dass die folgenden Ergebnisse erzielt werden:

1. Zeitnahe und zielgerichtete Benachrichtigung der Kunden
2. Analyse der betroffenen Servicekomponenten und Workflows
3. Gezielte Minderung der Auswirkungen von Vorfällen

In der letzten Phase, der **Phase der kontinuierlichen Verbesserung,** konzentriert sich das Team auf die Durchführung einer Post-Mortem-Analyse und die Lösung aller identifizierten Prozess-, Überwachungs-, Konfigurations- oder Codekorrekturen. Basierend auf dem Gesamtschweregrad und dem Risiko eines erneuten Auftretens werden die Korrekturen dann anhand des allgemeinen Engineering-Backlogs des Teams priorisiert.

2.10.1 Praktiken für die Serviceüberwachung

Das Business Central-Team von Microsoft legt Wert auf einen konsistenten, datengesteuerten und kundenorientierten Ansatz für den Betrieb seiner Live-Website. Die Definition von Service Level Indicators (SLIs) und die Implementierung von Live-Site-Monitoring-Warnungen sind Teil der Genehmigungskriterien für die Aktivierung einer neuen Business Central-Funktion in der Produktion. Produktgruppeningenieure umfassen auch Schritte zur Untersuchung und Minderung von Warnungen, wenn sie auftreten, mithilfe eines Vorlagen-Leitfadens zur Fehlerbehebung (Troubleshooting Guide, TSG).

Eine Möglichkeit, wie das Business Central-Team ein exponentielles Servicewachstum ermöglicht, ist der Einsatz eines DevOps-Teams. Diese Personen kennen sich mit Servicearchitektur, Automatisierung und Incident-Management-Praktiken aus und sind in Incidents eingebettet, um eine End-to-End-Lösung voranzutreiben. Das DevOps-Team verwendet ein Rotationsmodell, bei dem technische Führungskräfte aus der Produktgruppe für eine geplante Anzahl von Tagen die Rolle des Incident-Managers übernehmen. Das DevOps-Team stellt sicher, dass eine konsistente Gruppe von Personen Verbesserungen der Live-Website vorantreibt und Erkenntnisse aus früheren Vorfällen in zukünftige Eskalationen einfließen lässt.

Das DevOps-Team hilft auch bei groß angelegten Übungen, bei denen die Business Continuity and Disaster Recovery (BCDR)-Funktionen des Dienstes getestet werden.

DevOps-Praktiken erzwingen die Warnungsqualität auch auf verschiedene Weise:

1. Zu den TSGs gehören Folgenabschätzungen und Eskalationsrichtlinien
2. Warnungen werden so kurz wie möglich ausgeführt, um eine schnellere Erkennung zu ermöglichen
3. Warnungen verwenden Zuverlässigkeitsschwellenwerte anstelle von absoluten Grenzwerten, um Cluster unterschiedlicher Größe zu skalieren

2.10.2 Vorgehensweisen für die Reaktion auf Vorfälle

Wenn ein automatisierter Live-Site-Incident für Business Central erstellt wird, besteht eine der ersten Prioritäten darin, Kunden über potenzielle Auswirkungen zu informieren. Die Zielbenachrichtigungszeit von Azure beträgt 15 Minuten. Dieses Ziel kann je nach Anzahl der beteiligten Teams und Komplexität des Vorfalls schwer zu erreichen sein. In solchen Fällen besteht die Gefahr, dass die Kommunikation aufgrund der erforderlichen manuellen Analyse verspätet oder ungenau ist. Azure Monitoring bietet zentralisierte Überwachungs- und Warnungslösungen, mit denen Auswirkungen auf bestimmte Metriken innerhalb dieses Zeitfensters erkannt werden können.

Die Business Central Live-Site-Philosophie legt den Schwerpunkt auf die automatisierte Lösung von Vorfällen, um die allgemeine Skalierbarkeit und Nachhaltigkeit des Dienstes zu verbessern. Der Schwerpunkt auf Automatisierung ermöglicht eine Risikominderung in großem Maßstab und kann möglicherweise kostspielige Rollbacks oder riskante beschleunigte Korrekturen von Produktionssystemen vermeiden. Wenn eine manuelle Untersuchung erforderlich ist, verfolgt Business Central einen mehrstufigen Ansatz, bei dem die anfängliche Untersuchung von einem dedizierten DevOps-Team durchgeführt wird. DevOps-Teammitglieder sind erfahren in der Verwaltung von Live-Site-Incidents, der Erleichterung der teamübergreifenden Kommunikation und der Förderung der Risikominderung. In Fällen, in denen das amtierende DevOps-Teammitglied mehr Kontext zu einem betroffenen Szenario/einer betroffenen Komponente benötigt, kann es den Fachexperten (SME) dieses Bereichs um Beratung bitten. Schließlich führt das SME-Team Simulationen von Systemkomponentenfehlern durch, um Probleme im Vorfeld eines aktiven Vorfalls vor Ort zu verstehen und zu beheben.

Sobald die betroffene Komponente/das betroffene Szenario des Dienstes bestimmt ist, verfügt das Business Central-Team über mehrere Techniken, um die Auswirkungen schnell zu mindern. Im Folgenden sind einige der Techniken aufgeführt:

- **Aktivieren Sie die parallele Bereitstellungsinfrastruktur:** Business Central unterstützt die Ausführung verschiedener versionierter Workloads im selben Cluster. Auf diese Weise kann das Team eine neue (oder frühere) Version einer bestimmten Workload für bestimmte Kunden ausführen, ohne eine vollständige Bereitstellung (oder ein Rollback) auszulösen. Der Ansatz kann die Zeit für die Risikominderung verkürzen und das Gesamtrisiko der Bereitstellung senken.

- **BCDR-Prozess (Business Continuity/Disaster Recovery) ausführen:** Ermöglicht dem Team das Failover primärer Workloads in diese alternative Umgebung, in der Regel innerhalb von Minuten, wenn ein schwerwiegendes Problem in einer neuen Dienstversion auftritt. BCDR kann auch verwendet werden, wenn Umgebungsfaktoren oder abhängige Dienste den normalen Betrieb des primären Clusters/der primären Region verhindern.
- **Nutzen Sie die Resilienz abhängiger Dienste:** Business Central bewertet und investiert proaktiv in Resilienz und Redundanz für alle abhängigen Dienste (z. B. SQL und Key Vault). Die Resilienz umfasst eine ausreichende Komponentenüberwachung, um Upstream-/Downstream-Regressionen sowie lokale, zonale und regionale Redundanz (falls zutreffend) zu erkennen. Durch die Investition in diese Funktionen wird sichergestellt, dass Tools für das automatische oder manuelle Auslösen von Wiederherstellungsvorgängen vorhanden sind, um die Auswirkungen einer betroffenen Abhängigkeit zu verringern.

2.10.3 Praktiken zur kontinuierlichen Verbesserung

Das Business Central-Team überprüft alle Vorfälle, die sich auf den Kunden auswirken, während einer wöchentlichen Serviceüberprüfung. Alle Engineering-Gruppen, die zum Business Central-Service beitragen, nehmen an den Überprüfungen teil. Die Überprüfung gibt die wichtigsten Erkenntnisse aus dem Vorfall an Führungskräfte im gesamten Unternehmen weiter und bietet die Möglichkeit, unsere Prozesse anzupassen, um Lücken zu schließen und Ineffizienzen zu beheben.

Vor der Überprüfung bereitet das DevOps-Team Post-Mortem-Inhalte vor und identifiziert vorläufige Reparaturelemente für das Live-Site-Team und das Produktentwicklungsteam. Zu den Elementen können Codekorrekturen, erweiterte Telemetrie oder aktualisierte Warnungen/TSGs gehören. Business Central DevOps-Teams sind mit vielen dieser Bereiche vertraut. In der Regel nehmen sie die Anpassungen in Echtzeit vor, während sie auf einen aktiven Vorfall reagieren. Auf diese Weise wird sichergestellt, dass Änderungen rechtzeitig in das System integriert werden, um das erneute Auftreten eines ähnlichen Problems zu erkennen. Die detaillierte Analyse durch das Live-Site-Team hilft dem Produktentwicklungsteam, ein robusteres, skalierbareres und supportfähigeres Produkt zu entwerfen.

Neben der Überprüfung bestimmter Post-Mortems erstellt das Business Central-Team auch Berichte zu aggregierten Vorfalldaten, um Möglichkeiten zur Serviceverbesserung zu identifizieren, z. B. zukünftige Automatisierung der Incident-Minderung oder Produktkorrekturen. Die Berichterstellung kombiniert Daten aus mehreren Quellen, einschließlich des Kundensupportteams, automatisierter Warnungen und Servicetelemetrie. Die konsolidierte Ansicht bietet Einblick in die Probleme, die sich am negativsten auf den Service und die Gesundheit des Teams auswirken. Das Business Central-Team verwendet den Gesamt-ROI, um Verbesserungen zu priorisieren.

2.10.4 Release-Management- und Deployment-Prozess

Business Central veröffentlicht wöchentliche Funktionsupdates für den Dienst und gezielte On-Demand-Korrekturen, um Probleme mit der Servicequalität zu beheben. Der Ansatz

soll Geschwindigkeit und Sicherheit in Einklang bringen. Jede Codeänderung in Business Central durchläuft verschiedene Validierungsphasen, bevor sie auf breiter Basis für externe Kunden bereitgestellt wird.

Jede Änderung an der Business Central-Codebasis durchläuft automatisierte Komponenten- und End-to-End-Tests. Diese Tests validieren gängige Szenarien und stellen sicher, dass Interaktionen zu den erwarteten Ergebnissen führen. Darüber hinaus verwendet Business Central eine **CI/CD-Pipeline (Continuous Integration/Continuous Deployment**) in den Hauptentwicklungszweigen, um andere Probleme zu erkennen, deren Identifizierung pro Änderung unerschwinglich ist. Der CI/CD-Prozess löst einen vollständigen Cluster-Build und verschiedene synthetische Tests aus, die bestanden werden müssen, bevor eine Änderung in die nächste Phase des Release-Prozesses eintreten kann. Genehmigte CI/CD-Builds werden zur automatisierten und manuellen Validierung in internen Testumgebungen bereitgestellt, bevor sie in wöchentliche Funktionsupdates aufgenommen werden. Der Prozess bedeutet, dass eine Änderung innerhalb von 1 bis 7 Tagen nach Abschluss in eine mögliche Version integriert wird.

Ein Funktionsupdate durchläuft dann verschiedene offizielle Bereitstellungsringe des sicheren Bereitstellungsprozesses von Business Central. Der aktualisierte Produktbuild wird zuerst auf einem internen Cluster angewendet, der Inhalte für das Business Central-Team hostet, gefolgt von dem internen Cluster, den alle Mitarbeiter bei Microsoft verwenden. Die Änderungen warten in jeder dieser Umgebungen, bevor sie zum letzten Schritt übergehen: der Produktionsbereitstellung. Hier führt das Bereitstellungsteam einen schrittweisen Rollout-Prozess durch. Der Prozess wendet den neuen Build selektiv nach Region an, um eine Validierung in einer Region vor der breiten Anwendung zu ermöglichen.

Die Skalierung dieses Bereitstellungsmodells zur Bewältigung des exponentiellen Dienstwachstums erfolgt auf verschiedene Weise, wie in den folgenden Aufzählungszeichen beschrieben:

1. **Automatisierung**: Business Central-Bereitstellungen sind im Wesentlichen Zero-Touch, wobei das Bereitstellungsteam wenig bis gar keine Interaktion erfordert. Es gibt vordefinierte Rolloutspezifikationen für mehrere Bereitstellungsszenarien. Die Bereitstellungskonfiguration wird zur Buildzeit überprüft, um unerwartete Fehler während der Livebereitstellung zu vermeiden.
2. **Incident-Response-Prozess**: Bereitstellungsprobleme werden wie andere Live-Site-Incidents mithilfe von Techniken behandelt, die in den anderen Abschnitten dieses Artikels ausführlicher erläutert werden. Ingenieure analysieren Probleme mit dem Fokus auf sofortige Minderung. Anschließend folgen manuelle oder automatisierte Prozessänderungen, um ein erneutes Auftreten zu verhindern.
3. **Funktionsverwaltung**: Business Central wendet ein umfassendes Framework an, um Kunden selektiv neue Funktionen zur Verfügung zu stellen. Die Featureauslösung ist unabhängig von den Bereitstellungskadenzen. Es ermöglicht die Bereitstellung von Code für neue Szenarien in einem deaktivierten Zustand, bis er alle Qualitätsanforderungen erfüllt hat. Außerdem können neue Funktionen einer Teilmenge der gesamten Business Central-Population als zusätzlicher Validierungsschritt zur Verfügung gestellt werden, bevor sie global aktiviert werden. Wenn ein Problem

erkannt wird, können Sie mit dem Business Central-Funktionsverwaltungsdienst Funktionen in Sekundenschnelle deaktivieren, ohne auf zeitaufwändigere Rollback-Vorgänge für die Bereitstellung warten zu müssen.

2.11 SLA-Änderungen

Cloud-Services im Abonnement unterliegen einer permanenten Weiterentwicklung. Daher kann es notwendig sein, das SLA für Microsoft Onlinedienste anzupassen. Während der Vertragslaufzeit des Abonnements gilt die jeweils aktuelle Fassung der Servicebeschreibung, die hier https://learn.microsoft.com/en-us/dynamics365/business-central/dev-it-pro/service-overview abgerufen werden kann.

3 RELion ONE

RELion ONE ist eine Branchenlösung für das Immobilienmanagement auf Basis von Microsoft Dynamics 365 Business Central. Sie besteht aus mehreren Extensions zum MS Dynamics 365 Business Central-Standard.

Detaillierte Informationen zum immobilienwirtschaftlichen Funktionsumfang befinden sich in der Leistungsbeschreibung von RELion ONE.

Die Gesamtlösung, bestehend aus Business Central und den Extensions, wird als Service auf Basis von Microsoft Azure bereitgestellt, der via Browser erreichbar ist. Damit kann ein Anwender RELion ONE von jedem internetfähigen Endgerät mit modernem Browser nutzen. Details ergeben sich aus den jeweils

gültigen Systemvoraussetzungen von Microsoft für Business Central und sind in den Mindestanforderungen für die Nutzung von Business Central von Microsoft im Kapitel „Client Components" beschrieben (https://learn.microsoft.com/en-us/dynamics365/business-central/dev-itpro/deployment/system-requirements-business-central-v25).

3.1 Kompatibilität mit Business Central

RELion ONE ist eine Funktionserweiterung zum Online-Service Dynamics 365 Business Central von Microsoft. Die Parameter des Betriebs und Serviceleistungen von Microsoft sind in Kapitel 2 beschrieben. Ohne den Business Central Service ist RELion nicht nutzbar.

Die Auftragnehmerin stellt sicher, dass RELion ONE auf der jeweils von Microsoft bereitgestellte Version von Business Central lauffähig ist. Dabei werden die Entwicklungsrichtlinien von Microsoft beachtet. Vor der Freigabe eines neuen Releases prüft Microsoft automatisiert die technische Kompatibilität von RELion ONE mit der aktuellen Version von Business Central. Eine fachliche oder funktionale Prüfung übernimmt Microsoft nicht.

RELion ONE steht als „Extension" im „App-Source" von Microsoft für Business Central zur Verfügung. Die Auftragnehmerin stellt die jeweils geprüfte und freigegebene Version von RELion ONE dort bereit und Microsoft installiert diese automatisiert in der Plattform. Außerhalb des regelmäßigen Update-Turnus von Microsoft können Updates von RELion durch Administratoren des Kunden auch manuell installiert werden.

3.2 Fehlerbehebung und Wartung

Die Auftragnehmerin verfolgt für die Entwicklung von RELion ONE die gleichen Sicherheitsmaßnahmen und Regeln wie sie in Bezug auf Business Central in Kapitel 2 beschrieben werden. Durch intensive Tests soll vermieden werden, dass fehlerhafte Software zum Einsatz kommt. Sofern dies doch der Fall ist, wird je nach Schwere des Fehlers eine Korrektur mit dem nächsten planmäßigen Update oder ad-hoc veröffentlicht.

Gleichzeitig werden die Funktionen von RELion ONE gewartet, d.h. **bestehende** Funktionen werden an geänderte interne oder äußere Bedingungen angepasst. Dies können z.B. regulatorische Änderungen oder Formatänderungen beim Datenaustausch sein.

Wartungszeiten können vom Kunden in der Verwaltungsplattform (Dynamics 365 Business Central admin center) festgelegt werden (https://learn.microsoft.com/en-us/dynamics365/business-central/dev-itpro/administration/tenant-admin-center-update-management#set-the-update-window-for-each-environment).

3.3 Weiterentwicklung

RELion ONE wird kontinuierlich weiterentwickelt. Für die Branchenlösung RELion ONE werden derzeit monatliche Updates erstellt. Die Verfügbarkeit neuer Funktionen für einen Kunden hängt vom gewählten Leistungsmodell (Paket) ab. D.h. nicht jede neue Funktion wird in allen Leistungsmodellen bereitgestellt.

Im Zuge der Weiterentwicklung ist es zulässig, bestehende Funktionen zu verändern oder abzukündigen, wenn eine adäquate Alternative bereitgestellt wird.

4 Meldungen und Nachverfolgung

4.1 Meldungen

Jedes Problem im Zusammenhang mit dem Betrieb von RELion ONE wird als Meldung bei der Auftragnehmerin erfasst. Die Meldungen werden mit einem bestimmten Typ und einer Priorität klassifiziert, die auf Auswirkungen und Dringlichkeit basiert. Meldungen, die mit der Azure-Umgebung zusammenhängen, werden von der Auftragnehmerin entgegengenommen und an Microsoft zur Bearbeitung weitergeleitet. Jeder Typ wird gemäß dem beschriebenen Prozess behandelt. Jede Priorität hat eine festgelegte Reaktionszeit.

4.2 Erreichbarkeit und Arbeitsweise Service Desk

Der Service Desk ist über das Webportal seines IT-Service-Management-Systems (im Folgenden: ITSM-System) 24 Stunden am Tag erreichbar. Meldungen außerhalb des Servicezeiten (siehe 4.3 Nachverfolgung von Meldungen durch den Service Desk) werden am nächsten Werktag gemäß den in diesem SLA vereinbarten Reaktionszeiten bearbeitet. Der Kunde kann den Fortschritt der Bearbeitung über das Webportal des ITSM-Systems verfolgen.

Die Übermittlung von Meldungen kann nicht per E-Mail erfolgen, es sei denn, per E-Mail wird eine Verbindung zwischen dem ITSM-System des Aufragnehmers und einem anderen ITSM-System hergestellt.

Für den direkten Kontakt, zum Beispiel für dringende Benachrichtigungen, oder einfache Fragen, kann das Telefon genutzt werden.

Alle Meldungen werden als Ticket im ITSM-System protokolliert. Neben einem Thema und einer Erläuterung werden auch ein Tickettyp, Dringlichkeit, Auswirkungen und eine Produkt-Modul-Kombination erfasst. Der Kunde erhält eine Eingangsbestätigung mit der ihm zugewiesenen Ticketnummer. Der aktuelle Stand der Dinge kann jederzeit unter dieser Nummer angefordert werden. Basierend auf der Produkt-Modul-Kombination wird eine Benachrichtigung an die entsprechende Support-Gruppe weitergeleitet.

Meldungen können von den bei der Auftragnehmerin registrierten Kernnutzern und/oder funktionalen Administratoren des Kunden vorgenommen werden. Der Kunde wird diese im ITSM-System selbst erfassen oder der Auftragnehmerin zu diesem Zweck eine Liste zur Verfügung stellen, die die Namen, Anreden, Telefonnummern, E-Mail-Adressen und Rolle(n) innerhalb des ITSM-Systems der betreffenden Mitarbeiter enthält. Änderungen an dieser Liste können vom Kunden selbst im ITSM-System bearbeitet werden oder müssen vom Kunden schriftlich an den Service Desk mitgeteilt werden. Meldungen von nicht angemeldeten Mitarbeitern werden zurückverwiesen.

Vor der Erfassung eines Berichts im ITSM-System prüft der 1st-level-Support des Kunden die entsprechende Supportanfrage intern. Der Kunde ist hiermit für die Richtigkeit und Vollständigkeit der Mitteilung gemäß den in Anhang 2 dieses SLA enthaltenen Richtlinien verantwortlich. Nach der Validierung durch die Auftragnehmerin wird die Meldung bearbeitet. Wenn die bereitgestellten Informationen nicht ausreichen, wird die Meldung an den Kunden zurückgesandt. Meldungen, die auch nach Mahnung nicht den Richtlinien der Anlage 2 entsprechen, können von der Auftragnehmerin zurückgewiesen werden.

Nach der Validierung der Meldung wird sie in Übereinstimmung mit dem Prozess bearbeitet, der mit dem jeweiligen Tickettyp verbunden ist. Wenn möglich, wird der Service Desk die Meldung umgehend bearbeiten. Wenn die Meldung einem anderen Spezialisten gehört, wird er weitergeleitet.

Der Service Desk bietet 1st- und 2nd-Level-Support. Bei Bedarf kann der 2nd-Level-Support auf die Unterstützung von beispielsweise Produktspezialisten, Entwicklern oder Beratern zurückgreifen.

4.3 Nachverfolgung von Meldungen durch den Service Desk

Dem Kunden steht das Service Center als zentraler Ansprechpartner während der nachfolgend

ausgewiesenen Servicezeiten insbesondere für folgende Maßnahmen zur Verfügung:

- Entgegennahme von Fehlermeldungen und Kategorisierung von Anfragen, Problemen, Fehler- und Störungsmeldungen und
- Anforderungen (Anträge auf Änderungen)
- Auskunft über bekannte Fehler und Lösungsmöglichkeiten
- Behebung von Fehlern und Störungen (First- und Second Level Support)
- Weiterleitung von Tickets an den Second-Level Support
- Weiterleitung von Tickets im Bereich Azure-Betrieb an Microsoft

Das Service Center darf lediglich von den für Pflegeaufgaben zuständigen, vom Kunden zu benennenden

Key-Usern in Anspruch genommen werden. Bei einer Inanspruchnahme des Service Centers durch den Kunden wird die Auftragnehmerin den Vorgang erfassen und ihm eine neue Bearbeitungsnummer (Ticket) oder einen bereits in der Vergangenheit erfassten Bearbeitungsvorgang zuweisen.

Services	Servicezeiten
Servicezeiten (bedienter Betrieb)	Montag bis Donnerstag: 8.00 Uhr bis 17.00 Uhr MEZ bzw. MESZ
	Freitag: 8.00 Uhr bis 15.00 Uhr MEZ bzw. MESZ
	Mit Ausnahme bundesweiter Feiertage in Deutschland

Die Kontaktdaten des Service Desks sind in Anlage 1 (Kontaktdaten und Rollen im Service Desk) aufgeführt. Die Einzelheiten zur Bearbeitung von Meldungen erfolgen in Anlage 2 (Bearbeitung einer Meldung durch den Service Desk).

4.4 Service Desk

Service-Levels und -Verfahren

4.4.1 Service-Levels

Jedem Incident wird eine Priorität zugewiesen. In diesem Abschnitt werden die verschiedenen Service-Level für jede Priorität mit den angestrebten maximalen Reaktionszeiten

beschrieben. Die Auftragnehmerin wickelt alle Incidents so schnell und effizient wie möglich auf der Grundlage ihrer Priorität(en) ab.

Die Nichteinhaltung eines Service-Levels, die unter anderem durch einen der folgenden Gründe verursacht wird, fällt nicht in den Anwendungsbereich dieses SLA:

- Nichtrealisierung aufgrund höherer Gewalt. Z.B. ein physischer Ausfall im Microsoft Azure-Rechenzentrum. Dazu gehören Stromausfälle, Naturkatastrophen, vorübergehende Hardwareausfälle und ähnliche Ereignisse
- Nichtbeachtung, die durch den Kunden oder einen Dritten, dessen Handlungen der Auftragnehmerin nicht zuzurechnen sind, verursacht wurde.

Die Priorität eines Vorfalls wird auf der Grundlage von Auswirkungen und Dringlichkeit bestimmt, die bei der Registrierung ausgewählt werden können. Dabei spielen auch die Interpretation des "gesunden Menschenverstandes" und das betriebswirtschaftliche Bewusstsein des Service Desk-Mitarbeiters eine Rolle. Die folgende Tabelle enthält Richtlinien für die Vorfallindikatoren.

4.4.2 Reaktionszeit

Die Reaktionszeit ist die Zeit, die zwischen dem Eingang der Meldung des Kunden und dem Beginn der Serviceleistung liegt. Sie gilt nur innerhalb der definierten Servicezeiten. Die Reaktionszeit ist abhängig von der Priorität:

Priorität	Beschreibung	Reaktionszeit
0	Völliger Systemstillstand oder Störung der zentraler Funktionen mit hohen wirtschaftlichen Konsequenzen	15 Minuten
1	Fehlerhafte oder ausgefallene Funktionalität, die in der aktuellen Situation dringend benötigt wird; ernste Störung des gesamten produktiven Geschäftsablaufs	2 Arbeitsstunden
2	Fehlerhafte oder ausgefallene Funktionalität; Beeinträchtigung des normalen Geschäftsablaufs	10 Arbeitsstunden
3	Keine oder geringe Beeinträchtigung des normalen Geschäftsablaufs	14 Arbeitstage

4.4.3 Eskalationsstufen

Soweit in Anlage 5 nicht anders angegeben, gelten im Rahmen der Bearbeitung von Incidents folgende Eskalationsstufen:

Niveau	Kunde	Auftragnehmerin
0	Keyuser	Service-Desk
1	Funktions- und Systemmanagement	Teamleiter Service Desk / Serviceleiter
2	Leiter IT	Direktor / Geschäftsbereichsleiter
3	Geschäftsführung	Geschäftsführung

Vorfälle gehen auf Eskalationsstufe 0 ein. Im Falle eines Vorfalls der Priorität 0 wird dieser automatisch auf Stufe 1 eskaliert. In Situationen, in denen der Kunde der Meinung ist, dass keine ausreichenden Fortschritte erzielt werden und/oder mit einer ausgegebenen Liefererwartung nicht einverstanden ist, kann der Kunde auf Stufe 1 eskalieren.

Können sich der Kunde und die Auftragnehmerin nicht über die Priorisierung oder Behandlung eines Incidents einigen, kann der Incident auf eine höhere Ebene eskaliert werden.

4.4.4 Kundenbefragung

Der Zweck der Kundenbefragung ist es, die Qualität der Bearbeitung von Meldungen zu messen. Die Kundenbefragung wird regelmäßig durchgeführt. Dies geschieht, indem eine Stichprobe aller geschlossenen Meldungen des Vormonats genommen und nach Zufriedenheit gefragt wird. Sie werden nach ihrer Meinung zu Qualität, Lieferzeit, Lösungsangebot und Service von der Auftragnehmerin gefragt. Die Rückmeldung erfolgt durch die Berichterstattung über die Durchschnittsnote dieser Komponenten.

5 Zusätzliche Dienstleistungen

Unabhängig von diesem SLA oder anderen Verträgen kann der Kunde die Auftragnehmerin mit zusätzlichen Dienstleistungen beauftragen.

6 Kontaktdaten und Rollen im Service Desk

6.1 Kontaktdaten Service Desk

Webportal/Service Desk-Website: relion-service.aareon.com

6.2 Rollen im ITSM

Das aktuelle ITSM „Zendesk“ unterscheidet folgende Rollen:

- Endbenutzer: Mit dieser Rolle kann ein Mitarbeiter Berichte erstellen und eigene Berichte einsehen, diese Rolle wird neu hinzugefügten Mitarbeitern automatisch zugewiesen.
- Wichtiger Endbenutzer: Mit dieser Rolle kann ein Mitarbeiter Berichte erstellen und alle Unternehmensberichte einsehen.
- Produkt-Anforderer: Mit dieser Rolle können Softwareänderungen angefordert werden.
- Software-Empfänger: Diese Rolle wird für Software- und andere Updates per E-Mail verwendet.
- Kunden-Admin: Mit dieser Rolle können die Benutzer der eigenen Organisation gepflegt werden (Lagerung und Entsorgung und Wartung, Passwörter zurücksetzen und Rollen zuweisen).

6.3 Ticket-Arten

Das ITSM verwendet Tickettypen, um zwischen den verschiedenen Arten von Benachrichtigungen zu unterscheiden, die es gibt:

Ticket-Typ	Zu verwenden für
Vorfall	(Drohende) Störungen der vereinbarten Leistungserbringung
Benutzer-Hilfe	Fragen (hierfür ist der Abschluss eines gesonderten Support-Vertrags nötig)
Beratung	Anfragen für Beratung (hierfür ist der Abschluss eines gesonderten Support-Vertrags nötig)
Standard-Änderung	Standardisierte Anpassungen im Bereich der Benutzerverwaltung innerhalb der von der Auftragnehmerin gemanagten SaaS-Services.
Antrag auf Änderung	Anfragen im Rahmen der Dienstleistung des Funktionalen Managements oder nicht standardisierte Anpassungen an der von der Auftragnehmerin gehosteten Kundenumgebung
Produktanfrage	Anträge auf Funktionserweiterung der Software
Problem	Mehrere Vorfälle mit ähnlichen Symptomen oder ein einzelner Vorfall mit erheblichen Auswirkungen. In allen Fällen ist die Ursache noch unbekannt.

7 Einreichen einer Meldung an den Service Desk

Um eine Bearbeitung Ihrer Meldung zu ermöglichen, benötigen wir relevante Informationen. Je früher die erforderlichen Informationen verfügbar sind, desto schneller kann Ihre Meldung bearbeitet werden. Die folgenden Punkte bestimmen stark die endgültige Bearbeitungszeit Ihrer Benachrichtigung.

7.1 Meldung eines Problems (Funktionsstörung)

Beschreiben Sie klar und deutlich die Situation, in der das Problem auftritt.

1. Nennen Sie und die Fehlermeldung und die Funktion, bei der diese auftritt.
2. Erläutern Sie, welche Funktion ein fehlerhaftes Verhalten zeigt.
3. Welche Aktionen wurden in welcher Reihenfolge durchgeführt?
4. Fügen Sie der Meldung aussagefähige Screenshots bei.
5. Welche aktuellen Umstände könnten möglicherweise mit Ihrer Meldung zusammenhängen (Updates von RELion ONE oder in Ihrer lokalen Umgebung, wie Browser oder Betriebssystem des Clients, Firewall, Virenscanner, Zertifikate, sonstige Änderungen der Einrichtung, neue Daten)
6. Welcher Benutzer ist von dem Problem betroffen; betrifft es alle Benutzer?
7. Erarbeiten Sie, wenn möglich, ein konkretes Beispiel, um Ihr Problem zu verdeutlichen.
8. Erläutern Sie die Auswirkungen des Problems.

7.2 Meldung einer Performances-Störung

Wenn sich Ihre Meldung auf eine verminderte Performance (Antwortzeitverhalten) bezieht, möchten wir folgende Informationen erhalten:

1. Bei welcher Funktion oder Aktion tritt das Performanceproblem auf?
2. Tritt das Performanceproblem bei einer oder mehreren Funktionen auf?
3. Um welche Features oder Funktionalitäten handelt es sich?
4. Geben Sie an, wie die aktuelle Performance im Vergleich zu früheren Beobachtungen abschneidet.
5. Welcher Benutzer oder welche Benutzergruppe ist von diesem Performanceproblem betroffen?
6. Gibt es Performanceunterschiede zwischen diesen Benutzern und anderen Benutzern?
7. Ist die Performance zu bestimmten Tagen oder Tageszeiten reduziert?

7.3 Meldung einer Produktanfrage

- **Problemstellung**: Geben Sie deutlich an, in welchem Prozess Sie Probleme haben und wofür Sie nach einer Lösung suchen. Erarbeiten Sie, wenn möglich, ein konkretes Beispiel inklusive Screenshots, um Ihr Anliegen zu verdeutlichen.
- **Beschreibung der Änderung**: Beschreiben Sie die mögliche Lösung des Problems.
- **Begründung**: Erklären Sie deutlich, warum es ein Problem ist.
- **Risiken**, wenn der Anfrage nicht entsprochen wird: Beschreiben Sie die Risiken, wenn das Problem nicht gelöst wird.
- **Alternativen**: Beschreiben Sie die Alternativen zur Anforderung.

8 Performance-Überwachung

8.1 Azure Application Insights

Microsoft und die Auftragnehmerin (Aareon) nutzen Technologien zur Überwachung der Leistungsdaten der Services. In **Azure Application Insights** werden keine personenbezogenen Daten erhoben und gespeichert, sondern nur Daten zum Zwecke der Messung der Verfügbarkeit und/oder Leistung.

Welche Daten erhoben werden erfahren Sie unter Application Insights-Übersicht - Azure Monitor | Microsoft Learn.

8.2 Telemetrie

Umgebungen werden skaliert, um ein optimales Systemverhalten sicherzustellen. Dazu werden

Telemetriedaten erhoben, um die Performance der Anwendung und die Bearbeitungszeiten von SQL-Abfragen ermitteln zu können. Diese Telemetriedaten sind anonymisiert und beinhalten keine

personenbezogenen Daten. Die Speicherung erfolgt gemäß Richtlinien und Dokumentation von Microsoft (Monitoring and Analyzing Telemetry - Business Central | Microsoft Learn). Der Kunde kann selbst auf seine Telemetriedaten zugreifen und diese individuell im Dynamics 365 Business Central admin center einstellen.