IT-Sicherheitsstandards für Lieferanten

Hoher Sicherheitsgrad

ZWECK

Die IT-Sicherheitsstandards sollen Computacenter und die Daten ihrer Kunden dadurch effektiv schützen, dass sie ein flexibles aber dennoch einheitliches Konzept für das Management von Datensicherheit bieten und Computacenter's Anbieter helfen, die entsprechenden Sicherheitskontrollen besser zu verstehen und bei diesen mit Computacenter zusammenzuarbeiten. Computacenter's IT-Sicherheitsstandards für Anbieter beschreiben die Mindestanforderungen in Bezug auf Sicherheitskontrollen an ihre Anbieter, die eingehalten werden müssen. Sie beinhalten alle Aspekte, die für die Leistungserbringung für Computacenter oder deren Kunden relevant sind.

Anbieter müssen Computacenter‘s IT-Sicherheitsstandards überprüfen, sobald (a) erheblichen Änderungen im Betrieb des Anbieters in Kraft treten oder (b) mindestens alle zwei Jahre.

Alle neuen Anbieter sind verpflichtet, die geltenden Bedingungen dieser Standards, die die Leistungserbringung für Computacenter und deren Kunden betreffen, einzuhalten. Sollte ein direkter Konflikt zwischen den Anforderungen in diesen Standards und den Bedingungen aus einer schriftlichen Vereinbarung zwischen dem Anbieter und Computacenter bestehen, so haben die Bedingungen des schriftlichen Vertrags Vorrang, soweit diese den Konflikt betreffen.

GELTUNGSBEREICH

Diese Standards gelten für alle Lieferanten, die Zugriff auf Computacenter‘s Eigentum und Informationen oder die ihrer Kunden haben bzw. diese verarbeiten, einschließlich, jedoch nicht begrenzt auf:

- Lieferanten, die Informationen für Computacenter und deren Kunden verarbeiten, bereitstellen und übermitteln bzw. Zugriff auf diese haben
- den Zugriff auf die Computacenter-Umgebung von Remote-Standorten aus, an denen die IT-Einrichtungen nicht unter Computacenter‘s Kontrolle sind
- das Personal des Lieferanten, das Zugriff auf Informationen von Computacenter oder deren Kunden bzw. alle Bereiche der IT-Systeme benötigt.
    - Daher gilt dieser Standard für alle Mitarbeiter einschließlich Subunternehmer, Zeitarbeiter und andere Lieferanten, die direkt oder indirekt vom Lieferanten beauftragt werden.

1. INFORMATION SECURITY GOVERNANCE

Der Lieferant muss gewährleisten:

- dass er Personal ernannt hat, das die Gesamtverantwortung für das Informationssicherheitsprogramm des Unternehmens tragen und somit eine permanente Einhaltung in Bezug auf Computacenter‘s IT-Sicherheitsstandards gegeben ist.
- dass die Informationssicherheitsrichtlinien seiner Organisation erstellt, genehmigt, jährlich überprüft und an alle seine Mitarbeiter kommuniziert werden.
- dass er über einen Informationssicherheitsprozess verfügt, der aktiv genutzt wird, um die Wirksamkeit der Sicherheitsvorkehrungen zu überwachen und diese dem Führungsgremium des Lieferanten zu berichten.

2. COMPLIANCE UND WIRKSAMKEIT

Computacenter verpflichtet seine Lieferanten, Informationssicherheit zu gewährleisten und ihre dahin gehenden Anstrengungen bzw. die Wirksamkeit ihrer Maßnahmen nachzuweisen und Computacenter Belege darüber auf Anfrage vorzulegen. Dieser Nachweis erfolgt anhand einer vom Lieferanten durchgeführten Bewertung der Informationsrisiken & Sicherheitskontrollen.

- Alle Mitarbeiter des Lieferanten, die Services für Computacenter oder deren Kunden erbringen oder Zugriff auf Computacenter‘s Informationen bzw. Zutritt zu deren Standort(e) haben, müssen mindestens:

- allgemeine Best Practices in Bezug auf Informationssicherheit für alle gelieferten Komponenten und Materialien, einschließlich Software, Hardware und Informationen umsetzen, um die Vertraulichkeit, Verfügbarkeit und Integrität der Informationen von Computacenter und deren Kunden zu gewährleisten,
- Computacenter‘s Richtlinien zum angemessenen Umgang mit Informationen lesen, verstehen und einhalten,
- alle wertvollen und schützenswerten Informationen so klassifizieren und behandeln, wie dies in den Computacenter-Richtlinien dargelegt ist. Muss ein Lieferant bestimmte kundenseitige Sicherheitsrichtlinien einhalten, so lässt Computacenter ihm diese zukommen.

3. OUTSOURCING VON SERVICES AN DRITT- UND VIERTPARTEIEN

Der Lieferant ist nicht befugt, vertraglich festgelegte Services ganz oder teilweise ohne schriftliche Zustimmung von Computacenter an Dritt- oder Viertparteien zu übertragen. In Fällen, in denen Computacenter zugestimmt hat, dass bestimmte Aktivitäten vom Lieferanten an Subunternehmer übertragen werden, darf der Subunternehmer diese nicht ohne vorherige schriftliche Zustimmung von Computacenter weiter outsourcen.

Der Lieferant muss (im Rahmen seines Information-Security-Management-Konzeptes) gewährleisten, dass Lieferketten kontrolliert werden und Security-Compliance-Anforderungen wie vereinbart auf allen Ebenen der Lieferkette eingehalten werden. Nachweise über die Durchführung von Security-Compliance-Assessments für alle durch Drittparteien erbrachten Services, bei denen Computacenter‘s Informationen oder Informationen gespeichert oder verarbeitet werden, müssen Computacenter auf Anforderung vorgelegt werden (z.B. ISO27001-Akkreditierung, SOC-2 Reports).

4. MINIMIERUNG VON INFORMATIONSSICHERHEITSRISIKEN

Der Lieferant muss über ein Konzept zur Ermittlung von Informationssicherheitsrisiken verfügen, das geeignet ist, alle Risiken, die von seinen IT-Services verursacht werden, festzustellen und diese Computacenter‘s Information Security zu melden. Der Lieferant muss festgestellte Risiken umfassend dokumentieren und bewerten und entsprechende Schutzvorkehrungen treffen.

Darauf basierend muss der Lieferant gemeinsam mit Computacenter einen Sicherheitsplan bereitstellen, der genaue Angaben zu Schutzvorkehrungen gegen Risiken für Computacenter‘s Informationssicherheit und deren Wirksamkeit enthält. Der Lieferant übermittelt diese Risk Logs mit den ermittelten Sicherheitsrisiken für Computacenter und deren Kunden auf Anfrage und in einem angemessenen Zeitraum im Rahmen der vereinbarten Leistungserbringung.

5. IDENTITÄTSKONTROLLE, SICHERHEITSFREIGABE, SCREENING UND SICHERHEITSÜBERPRÜFUNG

Der Lieferant muss sicherstellen, dass alle seine Mitarbeiter, die:

- physischen Zutritt zu Geschäftsräumen von Computacenter und
- Remote-Zugriff auf die Informationen von Computacenter oder deren Kunden haben,

Computacenter‘s Richtlinien zum angemessenen Umgang mit Informationen und ggf. weitere lokale/ servicespezifische Richtlinien einhalten. Der Lieferanten muss alle Mitarbeiter bei Einstellung einer Zuverlässigkeitsprüfung unterziehen.

Computacenter führt, je nach Anforderungen, für bestimmte Positionen oder auf speziellen Kundenwunsch ggf. weitere Sicherheitsüberprüfungen des Personals des Lieferanten durch.

6. UNTERWEISUNG DES PERSONALS

Der Lieferant gewährleistet bei der Serviceerbringung für Computacenter oder deren Kunden, dass:

- eine Schulung zur Informationssicherheit ein Pflichtbestandteil bei der Einführung und im Schulungsprogramm für alle neuen oder bestehenden Mitarbeiter ist.
- alle Mitarbeiter über Bedrohungen und Bedenken bezüglich der Informationssicherheit informiert wurden, ihre Verantwortung und Pflichten kennen und in der Lage sind, den Sicherheitsrichtlinien Folge zu leisten.
- diese Schulungen und Einweisungen regelmäßig überprüft werden.

Computacenter kann von seinen Lieferanten verlangen, einen Bericht über den Stand der Schulungen für die Mitarbeiter, die Services für Computacenter und deren Kunden erbringen, vorzulegen.

7. SECURITY AUDIT

Computacenter muss nach angemessener Vorankündigung das Recht eingeräumt werden, Informationssicherheits-Audits entweder selbst oder durch einen vereinbarten externen Auditor durchzuführen, um die Einhaltung der Vereinbarung und Services, die am Lieferantenstandort erbracht werden, zu überprüfen. Audits werden zu vereinbarten Zeiten und in vereinbartem Umfang durchgeführt. Die Einhaltung der vertraglich vereinbarten Serviceanforderungen wird im Rahmen eines Audits geprüft. Die Ergebnisse des Audits müssen gemeinsam mit dem Lieferanten geprüft und dokumentiert werden.

Für den Fall, dass Unstimmigkeiten oder Abweichungen während der Bewertung der Sicherheitsrisiken und der Sicherheit oder während des Audits der vom Lieferanten erbrachten Services festgestellt werden, muss der Lieferant sicherstellen, dass angemessene Maßnahmen zur Risikominderung ergriffen und ein Korrekturplan zeitnah umgesetzt wird und Computacenter über deren Durchführung unterrichten.

8. BESCHAFFUNG, ENTWICKLUNG UND WARTUNG DER IT-SYSTEME UND SOFTWARE

8.1. SOFTWARE SERVICES

Bei der Erbringung von softwarebasierten Dienstleistungen für Computacenter oder deren Kunden, muss der Lieferant:

- mindestens berücksichtigen, dass die Software keine bekannten Fehler enthält, wie beispielsweise die in der neusten Version des “OWASP[1] (Open Web Application Security Project) aufgeführten Top Ten der gefährlichsten Schwachstellen bei Web- Anwendungen
- sich bemühen, die Best Practices aus dem OWASP (z.B. OWASP Test-Guidelines, OWASP Maturity-Modelle) zu übernehmen
- sicherstellen, dass er die branchenweit anerkannten Prozesse wie z.B. SDLC (Software Development Life Cycle) übernommen hat, um sowohl die Nutzbarkeit als auch die Gewährleistung zu garantieren
- garantieren, dass alle bereitgestellte / verwendete Software frei von schädlichen Codes (einschließlich Computerviren, Würmern, Logic Bombs, Hintertüren, Trojanern und sonstigen schädlichen Codes) ist, die die Sicherheit einer Anwendung beeinträchtigen können
- gewährleisten, dass er nur Software liefert, die unabhängig als geeignet verifiziert werden kann und keine allgemein bekannten Schachstellen enthält
- garantieren, dass alle Codes (einschließlich aller Codes von Drittparteien) vor ihrem Einsatz im Produktionsumfeld getestet wurden und eine lokale Kopie erstellt wurde und nicht nur darauf als eine separate Sammlung verweisen
- auf Anfrage von Computacenter Auskunft über sämtliche verwendete Software von Drittparteien einschließlich aller Libraries, Frameworks, Komponenten und anderer Produkte (kommerziell, frei, open-source oder closed-source) erteilen
- rechtzeitig Details zu End-of-Life-Produkten oder Services einschließlich Upgrade-Optionen liefern, damit Computacenter eventuelle Sicherheitsrisiken und mögliche Optionen der Risikobeseitigung abschätzen kann

Der Lieferant erklärt sich bereit, Computacenter‘s Review Team angemessen zu unterstützen und Source Codes zu liefern. Der Lieferant bietet Treuhandvereinbarungen für die Source Codes, die Computacenter nicht im Rahmen der Vereinbarung geliefert werden.

8.2. REMOTE-ZUGRIFF

Sollte der Lieferant einen Remote-Zugriff auf Computacenter‘s IT-Umgebung(en) benötigen, so verpflichtet er sich, folgende Standards bei der Leistungserbringung für Computacenter einzuhalten:

- Der Lieferant darf nur mithilfe des Remote-Access-Systems[2] auf Computacenter‘s IT-Umgebung(en) und nur im Rahmen der Erfüllung von vertraglichen Verpflichtungen in Bezug auf die Leistungserbringung für Computacenter zugreifen.

[1]Die Top Ten Sicherheitsrisiken für Web-Anwendungen sind hier zu finden: World Wide Web

[2]Zu Remote-Access-Systemen (RAS) zählen Computacenter‘s Partner Citrix Farm (PCF) oder CyberArk.

- Der Lieferant muss Sicherheitsmaßnahmen ergreifen, um seine IT-Umgebung vor Sicherheitsrisiken zu schützen (einschließlich Schwachstellen, Sicherheitsbedrohungen, Malware, Viren), die in einer Remote-Access-Lösung auftreten können[2].
- dieser zugriff über ein "Concierge"-Fernzugriffsmodell, durch "Screen-Sharing"[3] mit einem Computacenter-Mitarbeiter, der nur für den benötigten Zeitraum Zugriff auf das System gewährt,
- Der Lieferant muss effektive Sicherheitskontrollen (technisch, prozessual und organisatorisch) implementieren und durchführen, um die unerlaubte Verwendung seiner IT-Struktur zu verhindern und um alle User seiner IT-Infrastruktur gemäß Computacenter‘s Richtlinie zum Management von Benutzeridentitäten, Zugriff und Passwörtern identifizieren zu können.
- Die Nutzung ist nur für gültige Support-Incidents oder für genehmigte Change Requests erlaubt, die formell von Computacenter in den Support-Systemen des Lieferanten erstellt werden müssen[4].
- Der Lieferant muss Informationen gemäß der Matrix zur Klassifizierung und Handhabung von Informationen behandeln, wenn er Bildschirme (z.B. Microsoft Teams Session) mit Computacenter-Mitarbeitern teilt.
- Der Lieferant ist für alle Schritte bei der Verwendung solcher User Accounts in Computacenter‘s IT-Umgebungen verantwortlich.
- Das Personal des Lieferanten oder die Asset-Owner müssen eine Genehmigung einholen, wenn sie Software installieren möchten, mit der sie auf Computacenter‘s Remote-Access-System[2] zugreifen können. Computacenter ist weder im Besitz der Software, die für den Zugriff auf sein Remote-Access-System[2] erforderlich ist, noch bietet es Lizenzen oder Support dafür an.
- Computacenter behält sich das Recht vor, die Verwendung der Remote-Access-System-Lösung[2] in bestimmten Fällen ohne Vorankündigung zu untersagen oder auszusetzen. Computacenter bestätigt, dass die vereinbarten Service-Level für den Zeitraum, in dem der Lieferant die RAS-Lösung[2] infolge einer Aussetzung oder Deaktivierung nicht nutzen kann, nicht gelten.
- Die RAS-Lösung[2] kann genutzt werden, um Informationen von oder auf Computacenter‘s IT-Infrastruktur zu übertragen. Es ist dem Personal des Lieferanten untersagt, Informationen, die auf Computacenter‘s IT-Systemen gespeichert sind und Computacenter oder deren Kunden gehören, zu kopieren und / oder diese Informationen auf Geräte des Lieferanten oder andere Speicherorte außerhalb von Computacenter‘s IT-Infrastruktur ohne schriftliche Genehmigung durch Computacenter zu übertragen.
- Der Zugriff auf bzw. die Verwendung von Computacenter‘s Remote-Access-System[2] endet mit Beendigung der Vereinbarung mit dem Lieferanten.

8.3. ANFORDERUNGEN BEZÜGLICH INFORMATIONSAUSTAUSCH

- Lieferanten müssen stets eine vom Management freigegebene Unternehmensrichtlinie oder -richtlinien zur Informationssicherheit vorweisen können, die Verantwortlichkeiten und ein Informationssicherheitskonzept enthalten.
- Die Informationen von Computacenter oder deren Kunden werden gemäß den in Computacenter‘s Richtlinie zum angemessenen Umgang mit Informationen (Kapitel: Klassifizierung und Handhabung von Informationen / Matrix zur Klassifizierung und Handhabung von Informationen) festgelegten Kriterien klassifiziert. Die Anforderungen an die Sicherheit der Informationen, wenn diese elektronisch übermittelt oder gespeichert werden, richten sich nach der Klassifizierung.
- Computacenter und der Lieferant haben sich auf die geeignetste Methode des elektronischen Informationsaustauschs bei der Leistungserbringung für Computacenter oder deren Kunden geeinigt.
- Der Lieferant darf keine Informationen/Informationen von Computacenter oder deren Kunden ohne ausdrückliche Genehmigung durch Computacenter kopieren (weder in Papierform noch elektronisch).
    - die Genehmigung dazu muss in einem Information-Transfer-Log dokumentiert werden.

Hinweis: Die Herausgabe von Ad-hoc- und allgemeinen Geschäftskommunikationen ist hiervon ausgenommen.

8.4. LIEFERANTENNUTZUNG VON „CLOUD-BASIERTEN“ SERVICES ZUR INFORMATIONSVERARBEITUNG

- Die Speicherung und Verarbeitung von Computacenter-Informationen über Cloud-basierte Technology-Delivery-Plattformen (Infrastructure-as-a-service, Plattform-as-a-service, Software-as-a-service etc.) von Drittanbietern durch den Lieferanten muss gemäß den in diesem Dokument beschriebenen Sicherheitsanforderungen erfolgen.

[3] Screen-Sharing - Verwendung von Tools wie Microsoft Teams - Diese Methode ist notwendig, wenn eine bestimmte Sicherheitsfreigabe für den technischen Support erforderlich ist und die dritte Partei von einem entsprechend freigegebenen Computacenter-Mitarbeiter überwacht werden muss

[4] Zu den Support-System des Lieferanten zählen Service-Desk-Tools, um Incidents/Changes/Requests zu managen.

- Lieferanten, die Cloud-Services erbringen, müssen einen Prozess zur Vernichtung und sicheren Löschung von Computacenter's Informationen implementiert haben. Hierzu zählt auch ein Prozess zur Informations-Sanitisierung („Rücksetzung auf den Ursprungszustand" oder „Zeroing-out") von Speichern und das Entfernen von flüchtigen Informationen.
- Lieferanten, die Cloud-Services erbringen, müssen eine anerkannte Methode der Verschlüsselung sensibler Informationen bei der Speicherung und Übermittlung anwenden, die den Best Practices in der Branche entspricht.
- Lieferanten, die Cloud-Services erbringen, müssen Informationen und Assets von Computacenter oder deren Kunden sicher verwalten, indem sie diese logisch isolieren und sicher migrieren.
- Lieferanten, die Cloud-Services erbringen, müssen Konzepte oder Möglichkeiten zur Mehr-Faktor-Authentifizierung für Cloud-Administratorenrollen vorweisen können, die die Anforderungen von Computacenter oder deren Kunden erfüllen. Darüber hinaus erwartet Computacenter von Cloud-Service-Providern, dass sie Best Practices wie Mehr-Faktor-Authentifizierung bei der Zugriffskontrolle auf die Infrastruktur-Management-Systeme des Service-Providers anwenden.
- Lieferanten müssen Computacenter's Richtlinie zum Management von Benutzeridentitäten, Zugriff und Passwörtern und zum angemessenen Umgang mit Informationen einhalten.
- Lieferanten, die Cloud-Services erbringen, müssen dokumentierte Audits oder fundierte Compliance-Roadmaps vorweisen können, die den Standardzertifizierungen für Cloud-Sicherheit der Branche entsprechen (Beispiele hierfür sind ISO270017, NIST.SP.800-144, Cloud Computing Compliance Controls Catalogue (C5), CSA STAR, SSAE16, FEDRAMP, FIPS 140-2 und Open Data Alliance).
- Bei der Erbringung von Cloud-basierten Services muss nachgewiesen werden, dass diese die BC/DR[5]-Anforderungen erfüllen.
- Der Lieferant ist verpflichtet Computacenter mitzuteilen, wenn er Informationen außerhalb des europäischen Wirtschaftsraumes verarbeiten lässt.

8.5. SICHERHEIT DER IT-INFRASTRUKTUR DES LIEFERANTEN

Lieferanten müssen Computacenter's Sicherheitsstandards bei der Infrastruktur, die sie zur Leistungserbringung für Computacenter nutzen, einhalten.

- Lieferanten müssen über Standards und Prozesse verfügen, die im Rahmen eines dokumentierten Risk-Assessment-Prozesses die Vertraulichkeit, Integrität und Verfügbarkeit der Informationen und Services gewährleisten, permanent neue Bedrohungen und Schwachstellen überwachen und eine umgehende Risikobeseitigung erlauben.
- Lieferanten müssen ausreichende und umfassende Kontrollen für alle Sicherheitsaspekte, die sensible oder kritische Informationen oder die Informationsverarbeitung betreffen, implementiert haben, und diese müssen mittels Change Management, Schwachstellen-/Bedrohungsmanagement oder Information Security Incident Management gemanagt müssen.
- Der Lieferant muss einen End-Of-Life-Prozess (EOL) für alle Infrastrukturkomponenten definieren, der auch das EOL-Datum oder Business-Trigger berücksichtigen kann, die eine Änderung des EOL-Datums notwendig machen können.
- Alle sensiblen personenbezogenen Daten, die übermittelt werden, müssen sicher gespeichert werden. Das System darf keine personenbezogenen Daten in andere Systeme übertragen und nur für die angegebenen Zwecke genutzt werden, es sei denn, es liegt eine Genehmigung dazu von Computacenter oder den Informationseigentümern vor.
- Mit dem Internet verbundene Netzwerksegmente müssen durch Firewalls geschützt werden, die so konfiguriert werden müssen, dass sie alle dahinter liegenden Geräte vor allen bekannten Sicherheitsrisiken schützen.
- Anwendungen, Ports, Services o.ä. Zugriffspunkte, die auf einem Computer oder der Infrastruktur installiert sind und nicht unbedingt für die Leistungserbringung für Computacenter erforderlich sind, müssen deaktiviert oder entfernt werden.
- Bei allen Extranet-Verbindungen zu Computacenter muss es sich um von Computacenter genehmigte und autorisierte sichere Remote-Verbindungen handeln.
- Der Lieferant ist dafür verantwortlich, die sicheren Protokolle an seinen Standorten zu implementieren und diese über einen Change-Control-Prozess zu managen.
- Die Systeme müssen dazu in der Lage sein, potenzielle feindliche Angriffe zu entdecken. Hierzu zählen (sind aber nicht beschränkt auf): Network Intrusion Detection (NID) oder Host Intrusion Detection (HID) / Prevention. Alle Systeme müssen auf dem aktuellen Release-Stand sein und aktiv überwacht werden.
- Infrastrukturdiagramme, Dokumentationen und Konfigurationen müssen auf einem aktuellen Stand sein, kontrolliert werden und in der Lage sein, zur Problemlösung beizutragen.

[5] BC/DR = Business Continuity / Disaster Recovery

8.5.1. TRENNUNG VON MANDANTENFÄHIGEN INFRASTRUKTUREN UND ANWENDUNGEN

Computacenter ist bewusst, dass der Lieferant möglicherweise für mehrere Kunden Services erbringt. Daher müssen folgende Standards unter Verwendung entsprechender technologischer und organisatorischer Mittel eingehalten werden:

- Logische Trennung der IT-Systeme und Anwendungen, über die Services für Computacenter erbracht werden.
- Alle virtuellen Umgebungen, von denen aus Dienstleistungen für Computacenter erbracht werden, müssen durch strenge Zugriffskontrollen von denen der anderen Kunden des Lieferanten getrennt werden.
- Informationen in der technischen Architektur müssen den Anforderungen an die Informations-Sicherheitsarchitektur entsprechend getrennt gespeichert werden.
- Alle Elemente (einschließlich Einrichtungen und technische Infrastruktur), die für die Leistungserbringung für Computacenter erforderlich sind, müssen so weit wie möglich von denen der anderen Kunden des Lieferanten getrennt werden (physisch oder logisch).

8.5.2. TRENNUNG VON PRODUKTIONS-, TEST- UND ENTWICKLUNGSUMGEBUNG

- Der Lieferant muss gewährleisten, dass die Produktions-, Test- und Entwicklungsumgebung sowie die Produktions- und Test-Informationen während der Entwicklung und Erbringung einer vertraglich vereinbarten Dienstleistung getrennt werden (logisch und physisch).
- Es müssen Akzeptanzkriterien für neue Informationssysteme, Upgrades und neue Versionen aufgestellt werden und entsprechende Tests an dem/den System(en) während der Entwicklung und vor der Abnahme und Implementierung im Produktionsumfeld durchgeführt werden.
- Zugriffsrechte müssen durch entsprechende Gruppierungen und über das damit verbundene Rights Management kontrolliert werden, um die logische Trennung der Informationen einzelner Kunden zu gewährleisten.

8.5.3. AVAILABILITY MANAGEMENT; BACKUP MANAGEMENT

- Der Lieferant muss einen Availability-Management-Prozess implementieren, der die vereinbarten Service-Level / Security-Service-Level des für Computacenter oder deren Kunden erbrachten Services erfüllt.
- Um die Erreichbarkeit in Notfällen und bei Major Incidents / Ausfällen zu gewährleisten, müssen effektive Backup-Management-Pläne erstellt und das Recovery Management geplant und getestet werden.

8.5.4. ASSET & CONFIGURATION MANAGEMENT

- Es muss ein Asset-Register für die mit Computacenter vereinbarten vertraglichen Services angelegt und verwaltet werden.
- Der Lieferant stellt sicher, dass diese Informations-Assets nicht mit anderen geteilt werden, es sei denn, dies erfolgt im Einklang mit dem Computacenter-Prozess für die Erbringung der vertraglichen Leistung.
- Alle Assets, die für die Leistungserbringung für Computacenter genutzt werden, müssen sicher gelagert und vor unerlaubtem Zugriff, Veröffentlichung, Änderungen, Zerstörung oder sonstigen Eingriffen geschützt werden.
- Alle Informationen von Computacenter oder deren Kunden müssen auf Geräten gelöscht werden, bevor diese weiterverwendet werden dürfen.

8.5.5. OPERATIONS MONITORING, LOG & EVENT MANAGEMENT

- Es sollte ein automatisches Event-Reporting-System vorhanden sein.
- Audit-Logs, die User-Aktivitäten, Ausnahmen, und Informationssicherheits-Events aufzeichnen, müssen über einen vereinbarten Zeitraum aufbewahrt werden, um spätere Untersuchungen und die Zugriffsüberwachung zu erleichtern.
- Es muss technische Maßnahmen zur Systemüberwachung geben, um Security-System-Events zu erfassen.
- Sicherheitsrelevante Event-Logs von allen Komponenten der Infrastruktur müssen geprüft und entsprechende Maßnahmen ergriffen werden.
- Der Lieferant muss über einen Event-Management-Prozess verfügen, der dokumentiert und auf seine Funktionsweise hin getestet wurde, und der in der Lage ist, Cyber-Angriffe auf die erbrachten Lösungen und Services festzustellen.

8.5.6. CHANGE & RELEASE MANAGEMENT

- Der Lieferant muss gewährleisten, dass alle Änderungen bei den vertraglich vereinbarten Leistungen (einschließlich und nicht beschränkt Business Process Changes, IT Service Changes, Application/ Platform/Infrastructure Changes oder Änderungen an den zugrundeliegenden physischen und technischen Voraussetzungen) kontrollierbar sind und über einen formellen Change-Management-Prozess erfolgen.
- Changes, die die vertraglich vereinbarten Leistungen betreffen, müssen alle vorher angekündigt und von Computacenter genehmigt werden.
- Alle Freigaben von geänderten Services und Lösungen dürfen erst nach einem genehmigten Change Request und im Rahmen des formellen Release-Management-Prozesses des Lieferanten erfolgen.
- Die Online-Bereitstellung und automatische Verteilung von Software durch den Lieferanten muss im Einklang mit Computacenter‘s Informationssicherheits-Richtlinien erfolgen.

8.5.7. SCHWACHSTELLEN, PATCH MANAGEMENT UND PENETRATION TESTS

Der Lieferant muss über effektive Schwachstellen- und Patch-Management-Prozesse verfügen, um das Risiko zu minimieren, dass bekannte technische Schwachstellen ausgenutzt werden. Der Lieferant muss Computacenter‘s Richtlinie zum Management technischer Schwachstellen einhalten.

9. USER ACCOUNTS MANAGEMENT

9.1. AN- UND ABMELDUNG & ÜBERWACHUNG VON USERZUGRIFFEN

Lieferanten müssen ihre persönlichen User Accounts gemäß Computacenter‘s Richtlinie zum Management von Benutzeridentitäten Zugriff und Passwörtern und zum angemessenen Umgang mit Informationen verwalten. Im Speziellen, jedoch nicht ausschließlich wie folgt:

- Der Lieferant muss Computacenter‘s Prozess zur An- und Abmeldung seiner User zustimmen. Dies gilt sowohl für funktionale als auch für administrative/privilegierte Rollen. Der Prozess muss eingehalten werden, wenn Personal des Lieferanten auf Computacenter‘s IT-Umgebung zugreift.
- Der Lieferant muss über ein strenges Verfahren für das Management von neu eingestellten, intern wechselnden und ausscheidenden Mitarbeitern, die an der Serviceerbringung für Computacenter beteiligt sind, verfügen.
    - Die Accounts von neu eingestellten oder ausscheidenden Mitarbeitern müssen entsprechend gemanagt werden, um die Gefahr unerlaubter Zugriffe auf die Computacenter-Umgebung so gering wie möglich zu halten.
    - Wenn ein angemeldeter User den Lieferanten verlässt, muss der Lieferant gewährleisten, dass die entsprechende Useridentität sofort (innerhalb eines Arbeitstages) gesperrt wird und Computacenter‘s Access Management über die Änderung informieren.
- Der Lieferanten muss vierteljährlich die Liste mit den bei Computacenter registrierten Useridentitäten, ihre logischen Zugriffsrollen und Berechtigungen prüfen, um etwaige Abweichungen festzustellen und die Prüfergebnisse mit Computacenter abgleichen.

9.2. ROLLEN-BASIERTE LOGISCHE ZUGRIFFSKONTROLLEN, PRIVILEGIEN UND BEREITSTELLUNG

Als Teil der Servicebeschreibung wird ein Plan für die Rollen und Verantwortlichkeiten vereinbart. Die Rollen werden so festgelegt, dass Zugriffe nur so erfolgen können, wie sie gemäß den geschäftlichen Anforderungen erforderlich sind. Darüber hinaus werden administrative Rollen mit privilegierten Zugriffsrechten festgelegt und vereinbart.

- Der Lieferant muss die Rollen mit privilegierten Zugriffsrechten dokumentieren und nur Personal des Lieferanten mit den entsprechenden Rechten darf auf Computacenter‘s Informationen-Assets zugreifen.
- Der Lieferant muss ein Logging-Konzept für alle privilegierten Zugriffsrechte entwerfen und die Administatoren-Logs müssen Computacenter auf Anfrage vorgelegt werden.
- Bei Cloud-Services muss der Cloud-Anbieter die Anforderungen bezüglich Zugriffskontrollen für die Cloud-IT-Umgebung festlegen.

- Der Lieferant muss effektive Kontrollen aller privilegierten Zugriffe und das Log-Management aller privilegierten Aktivitäten auf bzw. in Betriebssystemen, Datenbanken, Middleware und geschäftlichen Anwendungen gewährleisten. Aktivitäten, die über einen privilegierten Zugriff erfolgen, müssen über das entsprechende Log-Management kontrolliert werden.

9.3. SICHERE ANMELDEPROZESSE

Der Lieferant muss für alle Accounts (einfach oder privilegiert) sichere Anmeldeprozesse unter Einhaltung anerkannter Branchenstandards bei der Authentifizierung und Autorisierung (z.B. Mahr-Faktor-Authentifizierung, keine Verwendung gemeinsam genutzter Anmeldeinformationen, automatisches Ablaufdatum) gewährleisten.

10. MOBILE DEVICE MANAGEMENT

- Der Lieferant muss garantieren, dass er über eine Richtlinie zum Schutz vor Risiken im Zusammenhang mit der Verwendung von mobilen Geräten, Telearbeit und Kommunikationsmitteln verfügt, sofern diese im Rahmen der Leistungserbringung für Computacenter oder deren Kunden genutzt werden.
- Der Lieferant und sein Personal müssen (sofern erforderlich) die entsprechenden Informationssicherheitsrichtlinien von Computacenter einhalten.

11. INCIDENT MANAGEMENT, REPORTING UND OFFENLEGUNG

- Der Lieferant muss ständig einen Incident-Management-Prozess pflegen, der Maßnahmen für das Management von Major Incidents oder Security Incidents beinhaltet.
- Es muss einen dokumentierten Incident-Management-Prozess zur physischen und Informationssicherheit (einschließlich Incident Response, funktionale und hierarchische Eskalation und Lösungsverfahren) geben.
- Das Personal des Lieferanten muss alle Security Incidents, Events und Schwachstellen zusammen mit allen wichtigen Details an die Kontaktperson bei Computacenter melden.
    - Incidents, Events und Schwachstellen müssen umgehend bei erster Gelegenheit und nicht später als 24 Stunden nach ihrem Auftreten gemeldet werden.
- Der Lieferant muss bei einem Sicherheitsverstoß umgehend seine Kontaktperson bei Computacenter informieren, da Computacenter möglicherweise rechtlich dazu verpflichtet ist, den Verstoß öffentlich bekanntzumachen oder weil andere Meldepflichten einzuhalten sind.
- Zu Information Security Events und Incidents zählen:
    - Totalausfall, Verlust von Equipment oder Anlagen,
    - Systemfehler oder -überlastung
    - menschliche Fehler
    - Verstoß gegen Richtlinien oder Vorgaben,
    - Verstoß gegen Vereinbarungen zur physischen Sicherheit,
    - unkontrollierte Systemänderungen,
    - defekte Hardware oder Software,
    - Verletzung von Zugriffsrechten
    - rechtliche und regulatorische Verstöße
    - Malware
    - Verdächtiges und vermeintlich harmloses Verhalten, das zu einem Event führen kann
- Der Lieferant muss für alle schwerwiegenden Major & Security Incidents Reporting-Prozesse an Computacenter vereinbaren und umsetzen, sofern diese die vertraglich festgelegten Servicevereinbarungen und die darin enthaltenen Security-Compliance-Level betreffen.
- Der Lieferant muss Computacenter umgehend über Ergebnisse und durchgeführte Changes im Zusammenhang mit festgestellten Fehlern und Schwachstellen bzw. nach der Behebung von Major & Security Incidents, die sich auf die Leistungserbringung auswirken, informieren.
- Beide Firmen handeln in Treu und Glauben bei der jeweiligen Beweissicherung und arbeiten, falls erforderlich, in zumutbarer Weise mit der jeweils anderen Firma bzw. den Behörden bei Untersuchungen zusammen.

12. SCHUTZ VOR MALWARE

- Der Lieferant muss auf allen seinen Systemen, die anfällig für Virusinfektionen sind, Antivirus-Lösungen implementiert haben.

- Drittparteien müssen angemessene Anstrengungen unternehmen, um versteckte Codes oder Informationen zu ermitteln, die folgende Ziele oder Auswirkungen haben:
    - Zerstörung, Änderung und Korruption von Computacenter-Informationen bzw. deren Diebstahl erleichtern
    - Deaktivierung oder Blockierung von Lieferanten- oder Computacenter-Systemen oder
    - Anwendung nicht dokumentierter oder genehmigter Zugriffsmethoden, um Zugriff auf Computacenter‘s Informationen bzw. die IT-Systeme des Lieferanten oder von Computacenter zu erlangen.
- Der Lieferant muss gewährleisten, dass der eingesetzte Malwareschutz:
    - auf dem neuesten Stand ist und es sich um eine unterstützte Version handelt;
    - mindestens einmal pro Tag mit Definitions- oder Signaturdateien aktualisiert wird;
    - On-Access- und On-Demand-Scans in Echtzeit erlaubt;
    - alle Inhalte scannt, die auf der IT-Infrastruktur, die Computacenter‘s Informationen verarbeitet, eingehen bzw. diese verlassen,
    - ist in der Lage, Malware zu desinfizieren, unter Quarantäne zu stellen oder zu löschen;
    - über Logging-, Warn- und Reporting-Funktionen verfügt,
    - nicht ausgeschaltet, neu konfiguriert oder von unautorisierten Usern deaktiviert werden kann.
- Der Lieferant muss gewährleisten, dass die Antivirus-Software und Antivirus-Definitionsdateien für alle Systeme des Lieferanten gemäß der branchenüblichen Best Practices und den Vorgaben des Herstellers der jeweiligen Antivirus-Software aktualisiert werden.
- Der Lieferant muss sicherstellen, dass die Geräte schädliche Codes, die sich auf ihnen befinden, entdecken, isolieren und beseitigen können.

13. INFORMATIONSVERSCHLÜSSELUNG UND KRYPTOGRAFIE MANAGEMENT

Ziel von kryptografischen Kontrollen (Verschlüsselung, digitale Zertifikate, digitale Signaturen) ist es, die Vertraulichkeit von Informationen zu gewährleisten bzw. deren unerlaubte Veröffentlichung zu verhindern, ihre Integrität zu bewahren (durch die Feststellung unerlaubter Änderungen), und deren Echtheit und Überprüfbarkeit zu gewährleisten (durch Nachweise, dass es sich bei dem Absender der Informationen auch tatsächlich um diesen handelt).

- Der Lieferant muss eine effektive Verschlüsselung von Informationen bei der Speicherung auf den Systemen gewährleisten. Es müssen sowohl Informationen, die sensible oder personenbezogene Informationen bei der Übertragung als auch alle sonstigen vertraulichen Informationen sowie von Computacenter vorgeschrieben verschlüsselt werden.
- Das Übertragungsmedium darf nur verwendet werden, wenn es ausreichend geschützt ist, es sei denn, es wurde von Computacenter‘s Information Security Management genehmigt.
- Der Lieferant muss über ein Konzept für einen umfassenden allgemeinen End-to-End-Management-Prozess verfügen einschließlich Erstellung, Verwendung, Speicherung und Zerstörung von Source-Keys.
    - Es müssen Überlegungen angestellt werden, wie diese allgemeinen Management-Praktiken zur Wiederherstellung von verschlüsselten Informationen genutzt werden können, falls ein Code unabsichtlich veröffentlicht oder zerstört wird bzw. verloren geht.
    - Der Lieferant muss gewährleisten, dass der Zugriff auf die Verschlüsselungscodes sicher und nur autorisiertem Personal vorbehalten ist. Die Codes selbst müssen physisch gesichert und der Zugriff darf erst nach Genehmigung durch mindestens zwei hierarchisch übergeordnete „Treuhänder“ erfolgen.

14. BUSINESS CONTINUITY MANAGEMENT & DISASTER RECOVERY PLANNING

Bei der Leistungserbringung für Computacenter oder deren Kunden muss der Lieferant die unten aufgeführten Standards zur Business Continuity (BC) und zum Disaster Recovery (RC) einhalten:

- Der Lieferant verspflichtet sich schriftlich an der Erstellung und Verwaltung eines ICT-Notfallplans nach ISO-22301- und ISO-27031-Standards mitzuwirken. Der verantwortliche Service Manager (Kontaktperson) des Lieferanten muss die erste Version des Notfallplans zusammen mit allen Updates an Computacenter zur Abstimmung übergeben und dessen Gültigkeit von Computacenter ausdrücklich schriftlich bestätigt werden.
- Der Lieferant muss gewährleisten, dass von seinem Senior Management abgezeichnete Business-Continuity-/Disaster-Recovery-Management-Pläne inklusive technischer und nicht-technischer Komponenten vorhanden sind und aktualisiert werden.
- Die BC/DR-Pläne müssen klare Informationen zu Workarounds und Gesamtwiederherstellungszeiten für die für Computacenter oder deren Kunden erbrachten Services enthalten.
- Während der BC/DR-Dauer muss der Lieferant Kommunikationskanäle mit Computacenter einrichten.
- Alle Mitarbeiter des Lieferanten, die an der Leistungserbringung beteiligt sind, müssen über die BR/DR-Pläne und ihre jeweilige Verantwortung während der BC/DR-Dauer aufgeklärt worden sein.

- Für alle Computacenter-Informationen muss ein Tool für regelmäßige Backups und mit Wiederherstellungsmöglichkeiten implementiert worden sein, das getestet wurde.
- Die Disaster-Recovery- und andere Ressourcen des Lieferanten müssen dokumentiert und Computacenter auf Anfrage vorgelegt werden.
- Darüber hinaus verpflichtet sich der Lieferant schriftlich, falls erforderlich, sich aktiv an Computacenter‘s Notfallmaßnahmen zu beteiligen, wozu auch Business-Continuity- und Recovery-Pläne zählen können.

15. VERTRAGSBEENDIGUNG; RÜCKGABE VON INFORMATIONEN UND INFORMATIONSVERARBEITENDEN ASSETS

Bei Beendigung der Servicevereinbarung zwischen dem Lieferanten und Computacenter muss Folgendes eingehalten werden:

- Computacenter und der Lieferant müssen rechtzeitig einen Exit-Management-Plan vereinbaren,
- die Exit-Management-Pläne müssen das Ende des für Computacenter erbrachten Service (einschließlich Cloud-basierte Services und/oder deren Rückgabe an Computacenter durch den jeweiligen Lieferanten) enthalten und in einem vereinbarten Format vorgelegt werden,
- der Lieferant muss alle Assets, die Eigentum von Computacenter sind, zurückgeben und die Zerstörung aller Informationen in seiner Umgebung sowie im Exit-Management-Plan beschrieben gewährleisten.

ANHANG A

Die relevanten Informationssicherheitsrichtlinien von Computacenter sind unten aufgeführt. Soweit zutreffend, werden dem Lieferanten die entsprechenden Richtlinien bei Bedarf zur Verfügung gestellt. Lieferanten, die z. B. im Auftrag von Computacenter vor Ort beim Kunden arbeiten, um vertragliche Verpflichtungen zu erfüllen, müssen sich an diese Richtlinien halten.

- Richtlinie zum angemessenen Umgang mit Informationen
- Richtlinie zum Management von Benutzeridentitäten, Zugriff und Passwörtern
- Richtlinie zum Management technischer Schwachstellen
- Richtlinie zum Malware-Schutz
- Richtlinie zur Netzwerk-Sicherheit
- Richtlinie zur Software-Sicherheit
- Richtlinie zur Endpoint-Sicherheit
- Richtlinie zur Überwachung von IT-Umgebungen
- Richtlinie zur Sicherheitsarchitektur
- Richtlinie zum IT Service Continuity Management
- Richtlinie zur Überwachung von Events und zum Logmanagement
- Richtlinie zur technischen Sicherheit der IT-Infrastruktur
- Richtlinie zur Physischen Sicherheit