IT-SICHERHEITSSTANDARDS FÜR ANBIETER
Mittlerer 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 Anbieter, die Zugriff auf Computacenter’s Eigentum und Daten oder die ihrer Kunden haben bzw. diese verarbeiten.

1. COMPLIANCE UND WIRKSAMKEIT

Computacenter verpflichtet seine Anbieter, Datensicherheit 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 durch den Anbieter durchgeführten Bewertung der Informationsrisiken & Sicherheitskontrollen.

Das Anbieterpersonal, das Leistungen für Computacenter oder deren Kunden erbringt, ist verpflichtet, die Richtlinien zum angemessenen Umgang mit Informationen einhalten.

2. PERSONAL (USER) MANAGEMENT

2.1. USER ACCOUNTS

Dem Personal des Anbieters werden ggf. User Accounts zur Verfügung gestellt, um auf Computacenter’s IT-Systeme und Anwendungen zugreifen zu können. Die Verwaltung dieser User Accounts muss gemäß Computacenter’s Richtlinie zum Management von Benutzeridentitäten, Zugriff und Passwörtern erfolgen.

- Der Anbieter muss Computacenter’s Prozess zur Registrierung und Abmeldung seiner User zustimmen. Dies gilt sowohl für funktionale als auch administrative/privilegierte Rollen. Dieser Prozess muss eingehalten werden, wenn Personal des Anbieters auf Computacenter’s IT-Umgebung zugreift.

- Der Anbieter muss ein strenges Verfahren für das Management neu eingestellter, intern wechselnder und ausscheidender Mitarbeiter, die an der Serviceerbringung für Computacenter beteiligt sind, implementiert haben.
    - Die Accounts von Mitarbeitern, die neu eingestellt werden oder die die Organisation verlassen, müssen so verwaltet werden, dass die Gefahr eines unerlaubten Zugriffs auf die Computacenter-Umgebung so gering wie möglich gehalten wird.
    - Wenn ein registrierter User den Anbieter verlässt, muss der Anbieter gewährleisten, dass die entsprechende Useridentität sofort (innerhalb eines Arbeitstages) gesperrt wird und Computacenter's Access Management über diese Änderung informieren.
- Der Anbieter muss eine vierteljährliche Prüfung der Listen mit den bei Computacenter registrierten Useridentitäten, ihrer logischen Zugriffsrollen und Genehmigungen durchführen, um etwaige Abweichungen festzustellen und die Prüfergebnisse mit Computacenter abgleichen.
- Die Mitarbeiter des Anbieters dürfen nach Kündigung der Vereinbarung mit Computacenter oder deren Kunden den/die User Account(s) nicht mehr verwenden.

2.2. NUTZUNG DES E-MAIL-SYSTEMS

Mitarbeiter des Anbieters können auf Vertrauensbasis eine Computacenter-E-mail-Adresse für geschäftliche Zwecke und gemäß Computacenter's Richtlinien zum angemessenen Umgang mit Informationen erhalten. Jeder Mitarbeiter muss die „Verpflichtungserklärung für Externe" lesen und unterschreiben, bevor Computacenter diese E-mail-Adresse zur Verfügung stellt.

2.3. IDENTITÄTSKONTROLLE, SCREENING UND SICHERHEITSÜBERPRÜFUNG

Der Anbieter muss Computacenter's Richtlinien zum angemessenen Umgang mit Informationen und ggf. weitere lokale / servicespezifische Richtlinien einhalten. Der Anbieter muss alle Mitarbeiter bei der Einstellung einer Sicherheitskontrolle (Pre-Engagement Screening) unterziehen.

Computacenter führt, je nach Anforderungen, für bestimmte Positionen oder auf speziellen Kundenwunsch ggf. weitere Backgroundchecks der Mitarbeiter des Anbieters durch.

2.4. ANWEISUNGEN UND VERHALTEN DER MITARBEITER DES ANBIETERS

Die Mitarbeiter des Anbieters müssen Computacenter's Richtlinien zur physischen Sicherheit und zur Überwachung von IT-Umgebungen einhalten. Der Anbieter muss gewährleisten, dass sein Servicepersonal (einschließlich Mitarbeiter oder Agenten seiner Subunternehmer) Computacenter's Geschäftsräume, Equipment oder Software nicht:

- zur Weiterleitung, Veröffentlichung oder Verbreitung von diffamierenden, anstößigen, beleidigenden, obszönen oder bedrohenden Inhalten nutzt;
- so nutzt, dass es Persönlichkeitsrechte von Personen, Firmen oder Unternehmen verletzt (einschließlich, jedoch nicht beschränkt auf Urheberrechte oder Schweigepflicht) oder
- für persönliche Zwecke nutzt

und dass sein Personal im erforderlichen Umfang über die sich aus Computacenter's Datenschutzrichtlinien ergebenden Anforderungen informiert wurde und diese befolgt.

Inakzeptables Verhalten bei der Ausführung von vertraglich vereinbarten Aktivitäten kann zu einem Verweis vom Firmengelände führen und die betreffenden Personen werden dem Supplier Management Team gemeldet. Sicherheitsverstöße seitens der Mitarbeiter des Anbieters ziehen einen formellen disziplinarischen Prozess nach sich.

2.5. UNTERWEISUNG DES ANBIETERPERSONALS

Der Anbieter gewährleistet, dass alle seine Mitarbeiter, die für Computacenter oder deren Kunden arbeiten, eine entsprechende Aufklärungsschulung zur Datensicherheit erhalten haben. Diese Schulung muss zum Einstellungszeitpunkt im Rahmen der Einarbeitung erfolgen und während der Vertragslaufzeit für alle Mitarbeiter nochmals als Auffrischungsschulung durchgeführt werden.

3. IT-EQUIPMENT-MANAGEMENT

3.1. VERWENDUNG VON IT-EQUIPMENT UND EIGENTUM

Dem Anbieterpersonal wird ggf. IT-Equipment oder anderes Eigentum von Computacenter zur Verfügung gestellt. Hierzu zählen: Zwei-Faktor-Authentifizierungs-Token, Mitarbeiterausweise mit Foto, PCs und Laptops. Wechselspeicher (z.B. verschlüsselte USB-Sticks) sind verboten, es sei denn, es liegt eine schriftliche Genehmigung für deren Verwendung von Computacenter vor. Das Anbieterpersonal muss sämtliches Equipment auf Anforderung an Computacenter zurückgeben und Computacenter's IS Service Desk umgehend über verlorenes oder gestohlenes Equipment informieren. Der IT Service Desk kann rund um die Uhr an 365 Tagen im Jahr unter den folgenden Telefonnummern kontaktiert werden:

- +44 (0)1707 631111 (UK)
- +49 2273 597 7777 (DE)
- +33 148 176 99 (FR)

Sollte Kundenequipment, das von Computacenter an Mitarbeiter des Anbieters ausgegeben wurde, verloren gegangen oder gestohlen worden sein, so muss dies dem Sponsor/der Kontaktperson bei Computacenter sofort gemeldet werden, um sicherzustellen, dass entsprechende Maßnahmen ergriffen werden können und der Kunde darüber informiert wird. Der Kunde sollte darüber nur durch den zuständigen Computacenter-Service-Manager bzw. die Kontaktperson informiert werden.

Sämtliches IT-Equipment, das von Computacenter zur Verfügung gestellt wurde (z.B. Laptop, PC, Handy) und das Daten von Computacenter oder deren Kunden enthält, muss beim Transport außerhalb der Geschäftsräume des Anbieters gegen widerrechtliche Zugriffe, Missbrauch oder Zerstörung geschützt werden, soweit dies praktisch umsetzbar ist. IT-Equipment, Datenträger oder Daten dürfen die Geschäftsräume des Subunternehmers nicht ohne Genehmigung verlassen.

3.2. VERWENDUNG VON IT-EQUIPMENT, DAS NICHT COMPUTACENTER GEHÖRT

IT-Equipment, das nicht Computacenter gehört (d.h. persönliches oder privates Equipment), darf bei der Erbringung von Services für Computacenter oder deren Kunden nicht verwendet werden. Hierzu zählt auch die Verwendung privater Smartphones, Tablets und PDA-Geräte, auf die Daten kopiert und / oder gespeichert werden können.

3.3. REMOTE-ZUGRIFF

Sollte der Anbieter einen Remote-Zugriff auf Computacenter's IT-Umgebung benötigen, so darf:

- dieser zugriff über die spezifischen Benutzerkonten, die ihnen von Computacenter zur Verfügung gestellt werden,

- dieser zugriff über ein "Concierge"-Fernzugriffsmodell, durch "Screen-Sharing[1]" mit einem Computacenter-Mitarbeiter, der nur für den benötigten Zeitraum Zugriff auf das System gewährt,
- dieser spezielle User Account nur für den Zweck verwendet werden, für den er zur Verfügung gestellt wurde, wobei dieser Zweck in einem Incident/Request/Change Record dokumentiert werden muss,
- und es dürfen keine Informationen/Daten ohne ausdrückliche Genehmigung von Computacenter kopiert werden (weder in Papierform noch elektronisch).

4. INCIDENT MANAGEMENT, REPORTING UND AUSKUNFT

Das Anbieterpersonal muss alle Security Incidents, Events und Schwachstellen zusammen mit allen wichtigen Details an ihre Kontaktperson bei Computacenter melden. Incidents, Events und Schwachstellen müssen umgehend und dürfen nicht später als 24 Stunden nach ihrem Auftreten gemeldet werden.

Der Anbieter muss bei einem Sicherheitsverstoß umgehend seine Kontaktperson bei Computacenter informieren, da Computacenter möglicherweise rechtlich dazu verpflichtet ist, den Verstoß öffentlich bekannt zu machen oder andere Meldepflichten einzuhalten sind.

Der Anbieter muss Computacenter umgehend bei vermuteten oder tatsächlichen Verletzungen der Geheimhaltungspflicht und über die Computacenter-User-Accounts, von denen diese begangen wurden, informieren.

ANHANG

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 zur Physischen Sicherheit

[1] 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.