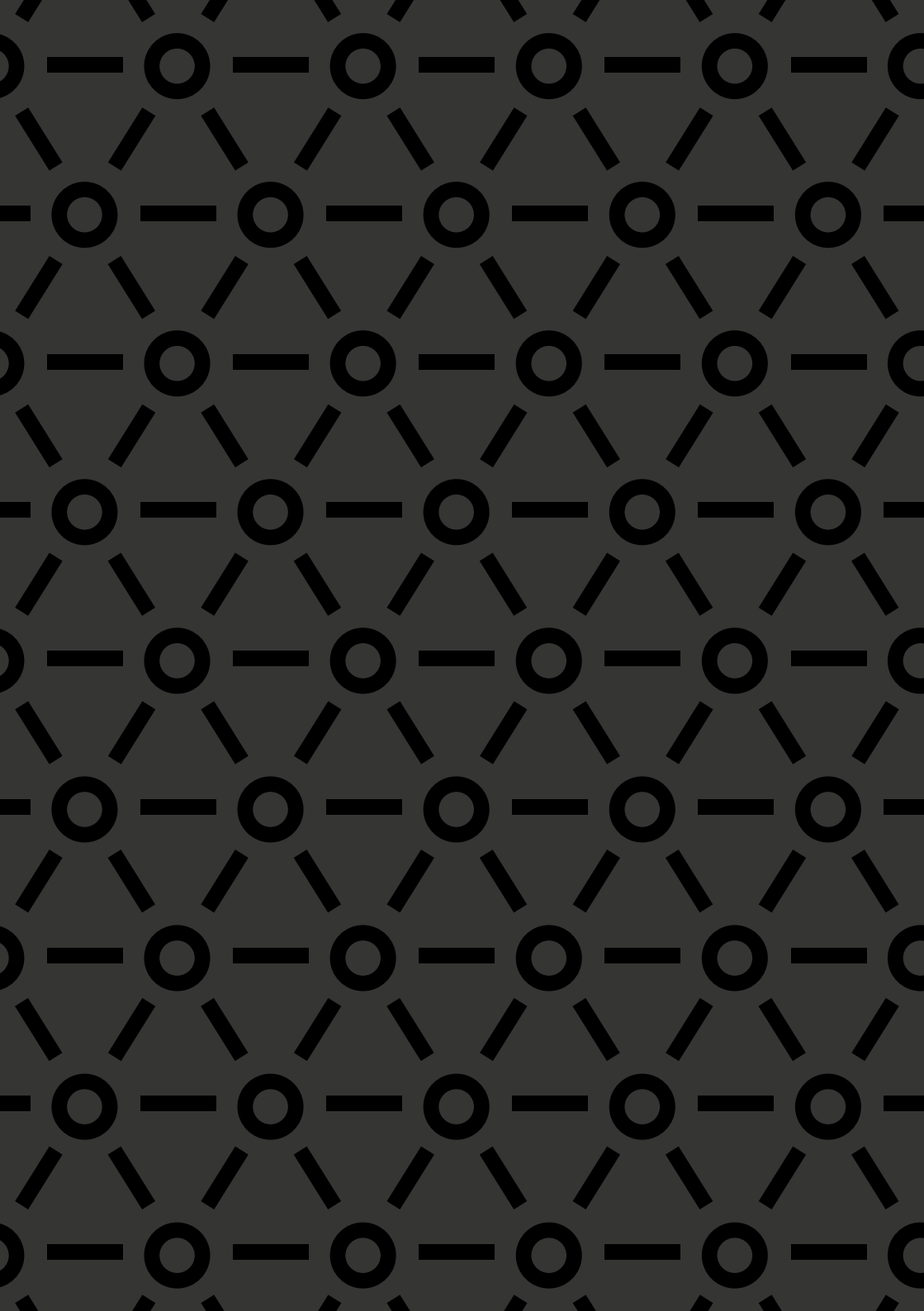
e–shelter
security

— Data Center Whitepaper

Multifunktionale Ansätze für die Entwicklung von Rechenzentren



— Inhalt

— Einleitung

Die Struktur von Rechenzentren hat sich in den letzten Jahren stark verändert. Noch vor wenigen Jahren betrieb fast jedes Unternehmen seine eigene IT-Landschaft, in der individuell angepasste Systeme intern entwickelte Software ausführten. Waren Rechenzentren früher eine versteckte Einrichtung im Untergeschoss des Unternehmenssitzes oder in einem eigenen geheimen Gebäude, entstehen heute große Rechenzentrumsareale mit mehreren spezialisierten und gut gesicherten Gebäuden.

Diese Standorte bauen auf einer einheitlichen Infrastruktur auf, um viele verschiedene Kunden zu unterstützen. Fortschrittliche Kommunikationstechniken ermöglichen aus zentralen Megastandorten die Bereitstellung standardisierter und zuverlässiger Cloud-Dienstleistungen wie etwa Software as a Service. Infolgedessen bevorzugen immer mehr Unternehmen externe Anbieter, um die Abhängigkeit von ihren internen Systemen (und deren Wartungsaufwände) zu verringern, flexibler zu werden, Kosten zu sparen und sich mehr auf ihre Kernkompetenzen zu konzentrieren.

Die Betreiber von Rechenzentren stehen vor besonderen Herausforderungen. Während der Ausfall eines unternehmensinternen Rechenzentrums nur den Geschäftsbetrieb dieses einen Unternehmens betrifft, muss ein Multi-Tenant-Rechenzentrum für viele Kunden die Verfügbarkeit und Sicherheit aufrechterhalten. Je nach tatsächlicher Lieferkette von Rechenzentren, Cloud- und IT-Dienstleistern und Kommunikationsnetzbetreibern ist das Abhängigkeitsschema komplexer sowie erfordert neue Definitionen für Service, Sicherheit und Verfügbarkeit: Die Ziele müssen so gesetzt werden, dass nicht nur die Anforderungen eines einzelnen Unternehmens erfüllt werden, sondern eine Vielzahl an Diensten zur Unterstützung verschiedener Kunden aus unterschiedlichen Branchen zur Verfügung steht, die zudem unterschiedlichen gesetzlichen und regulatorischen Anforderungen genügen.

— Anforderungen für große Service-Rechenzentren

Neue Rechenzentrumsstandorte sollen möglichst in der Nähe von Wirtschaftszentren entwickelt werden, mit einer ausreichenden Nachfrage nach IT-Diensten, die eine sichere und verfügbare Infrastruktur erfordern. Gerade „Hyperscaler", große und global agierende Unternehmen, die verschiedene Arten von Cloud-Diensten anbieten, haben strenge Anforderungen an die Betreiber von Rechenzentren. Sie sollen eine hohe Servicequalität zu einem günstigen Preis bereitstellen.

Während einige Unternehmen versuchen, sich auf Standorte in Ländern mit niedrigen Energiekosten, erschwinglichen Immobilien und Zugang zu internationalen Datennetzen zu konzentrieren, wollen andere Anbieter nah am Kunden sein. Gesetzliche Rahmenbedingungen und die Forderung nach ultraschnellen Reaktionszeiten verlangen nach Standorten in der Nähe von Wirtschaftszentren, wo Platz und Energie[1] knapp und entsprechend teuer sein können. Wichtig sind für viele Unternehmen Lagen, an denen die Datennetze leistungsstark und die Entfernungen gering sind sowie die gesetzlichen Rahmenbedingungen denen der Kunden entsprechen. Die Identifizierung von Grundstücken, die den Anforderungen von Rechenzentrumsbetreibern und deren Kunden entsprechen, ist eine Aufgabe für Experten mit einem hohen Maß an lokalen Kompetenzen. Diese Fachleute sind bei der Identifizierung solcher Grundstücke, der Analyse der Umweltsituation, der Planung von Risikominderungen und der Beachtung der lokalen Vorschriften, die einen großen Einfluss auf die Gestaltung des Rechenzentrums haben können, besonders wertvoll.

Experten analysieren systematisch:

— natürliche Risiken, wie potenzielle Quellen für Überschwemmungen, extreme Temperaturen, Starkregen, Stürme, Erdbebenaktivität und andere Umgebungsbedingungen, unterirdische Strukturen oder Bodenkontaminationen, Gebäude und Betriebe in der Umgebung, industrielle Risiken durch nahe gelegene Fabriken, insbesondere Prozessindustrie, die mit großen Mengen von entflammbaren, explosiven, potenziell toxischen oder nuklearen Materialien arbeiten, Quellen von elektromagnetischer Strahlung, verkehrsbedingte Risiken wie große Straßen, Güterzugstrecken oder Flugverkehr,
— Ziele, welche Verkehrsstaus, Demonstrationen oder andere große Versammlungen verursachen könnten,
— soziale Situation und kriminelle Brennpunkte,
— sonstige individuelle Risiken, die den Betrieb oder auch den Zugang zum Rechenzentrumsbereich beeinträchtigen könnten.

Eine Umfeldanalyse, die standortgerechte physische Sicherheits- und Verfügbarkeitsmaßnahmen definiert, zählt zu den wichtigsten Anforderungen.

Kunden werden nach dem Grad der Kontrolle fragen, den das Rechenzentrum bietet, wie z. B.:
— Welche Maßnahmen wurden umgesetzt, um den für den Standort identifizierten Risiken entgegenzuwirken?
— Wie hoch ist der Grad der Resistenz gegen Angriffe von außen?
— Wie wird der Zugang zum Standort überwacht, um zu gewährleisten, dass nur autorisierte Personen kritische Bereiche betreten?

[1] Die Gemeinden Amsterdam und Haarlemmermeer haben beispielsweise die Entwicklung neuer Rechenzentren aufgrund von Überlegungen zur Energieverfügbarkeit und Umweltbelastung im Jahr 2019 gestoppt – siehe https://www.amsterdam.nl/nieuwsarchief/persberichten/2019/persberichten-marieke-doorninck/regie-vestiging-datacentersamsterdam/ - eine Richtlinie für eine selektive Wachstumspolitik im Jahr 2020 veröffentlicht, siehe https://www.amsterdam.nl/bestuur-organisatie/college/wethouder/marieke-doorninck/persberichten/amsterdam-selectievegroei-datacenters/

— Verfügbarkeit von Rechenzentren

Rechenzentrumsbetreiber stellen als Kernleistungen widerstandsfähige und solide Gebäude, hochverfügbare Infrastruktur für Stromversorgung, Kühlung und Luftaufbereitung, Sicherheit für den Zugriffsschutz und zuverlässige Prozesse für das Zugriffsmanagement bereit. Darüber hinaus werden Netzwerkdienste benötigt. Je nach Geschäftsmodell kann ein Betreiber den Zugang zu passiven Netzwerken zur Verfügung stellen oder auch die aktive Vermittlung von logischen Netzwerken innerhalb des Rechenzentrums, zu anderen Gebäuden oder Standorten, dem Internet oder Cloud-Anbietern übernehmen.

Verschiedene Institutionen haben normative Rahmenwerke für die Ausfallsicherheit von Rechenzentren geschaffen. Das Uptime Institute hat die Tier-Spezifikationen veröffentlicht, die Telecommunications Industry Association (TIA) beschreibt in der TIA942 Bewertungsstufen, und die CENELEC hat die Norm EN 50600 erstellt, um nur einige zu nennen. Alle drei Institutionen haben vier Stufen der Verfügbarkeit mit ähnlichen, aber nicht identischen Kriterien und Erweiterungen definiert. Typischerweise gibt die niedrigste Stufe die Mindestanforderungen an die Infrastruktur von Rechenzentren vor, während die höchste Stufe die „perfekte" Lösung ohne Single Point of Failure beschreibt. Aber „perfekt" heißt auch „teuer". Das ausfallsicherste Rechenzentrum anbieten zu können hat nicht zwingend zur Folge, dass die Kunden den dafür entsprechenden Preis zahlen wollen. Somit muss das Design eines Rechenzentrums und seiner Infrastruktur sorgfältig gestaltet werden, um den Anforderungen der Kunden zu entsprechen und das beste Preis-Leistungs-Verhältnis zu bieten.

Ebenso wichtig sind externe Faktoren:

— Wie zuverlässig ist die externe Stromversorgung?
— Wie viel Strom kann ich jetzt und in Zukunft nutzen, wenn mein Bedarf steigt, aber die Versorgungsnetz- oder Verbundnetz-Kapazitäten eventuell begrenzt sind?
— Was brauche ich, um Stromausfälle zu vermeiden?
— Sind Dieselgeneratoren immer noch die erste Wahl oder sollte ich andere Technologien, wie z. B. Brennstoffzellen, in Betracht ziehen?
— Wie hoch dürfen die Emissionen sein, wenn meine Generatoren Lärm und Abgase produzieren?
— Welche Kapazitäten sind im Datennetz verfügbar? Habe ich jetzt und in Zukunft genügend Kapazitäten? Sind die Netzwerkepfade redundant oder gibt es Single Points of Failure?
— Sind meine Lieferanten und Wartungsfirmen schnell verfügbar, wenn ich Unterstützung benötige, z. B. bei Störfällen, aber auch für die regelmäßigen Wartungsarbeiten?
— Werden kritische Ersatzteile in ausreichender Zahl vorgehalten und sind sie schnell verfügbar, um unmittelbar reagieren zu können?

Kritisch sind Stromnetzbetreiber und Treibstofflieferanten für den Notbetrieb. Der Treibstoff für Notstromanlagen ist begrenzt, die Logistik für die Nachlieferung kann aufwendig und eine Lieferung an Feiertagen oder Wochenenden unmöglich sein.

Sie sollten sicher sein, dass Sie gut investieren und qualifizierte Ingenieure und Experten an Ihrer Seite wissen, bevor Sie diese wichtigen Entscheidungen treffen.

— Nachhaltigkeit

100 % der in einem Rechenzentrum verbrauchten Energie wird letztlich in Abwärme umgewandelt. Die vom Netz gelieferte Energie stammt aus einem Mix erneuerbarer, fossiler und nuklearer Quellen. Viele Kunden haben Programme aufgelegt, um klimaneutral zu werden, und Rechenzentren müssen diesen Trend unterstützen. Hier sind Konzepte gefragt, die den Einsatz von erneuerbaren Energien maximieren, aber auch die Betriebskosten senken und den Bedarf der IT-Systeme im Rechenzentrum minimieren.

Da der überwiegende Teil der Abwärme bei recht niedrigen Temperaturen entsteht und deshalb eine Wiederverwendung, z. B. zur Beheizung von Häusern, schwierig ist, sind umfassendere Ansätze nötig. Der Einsatz von dezentraler Energieerzeugung, Gleichstromtechnik oder Hochtemperaturprozessoren kann helfen, die Effizienz zu steigern. Die benötigten Systeme bieten Hersteller jedoch noch nicht in großen Stückzahlen und zu erschwinglichen Preisen an.

Umweltauswirkungen sind ein wichtiger Aspekt der Nachhaltigkeit. Aber auch Themen wie die Umfeldeingliederung, die Ausgewogenheit von Investitionen und Wert des Betriebs - nicht nur für die Eigentümer, sondern auch für die Gesellschaft spielen eine Rolle. Wie sind die Arbeitsbedingungen im Rechenzentrum und in der Lieferkette? Wird das Unternehmen seiner sozialen Verantwortung gerecht? Immer mehr Kunden verlangen einen Nachweis über Nachhaltigkeitsprinzipien, die von ihren Lieferanten umgesetzt werden - und Rechenzentren sind Teil der meisten Lieferketten.

— Sicherheit, Zutrittsschutz und Zutrittsmanagement

Nur autorisiertes Personal darf Zutritt zum Rechenzentrum erhalten. Mit der heute verfügbaren Technologie kann der Schutz eines Rechenzentrums weitgehend zu einem automatisierten Prozess werden. „Intelligente" Zäune mit Videoüberwachung können auf ein sehr hohes Widerstandsniveau ausgelegt werden. Angreifer oder Eindringlinge werden frühzeitig erkannt. Zudem schützt es vor gewaltsameren Angriffen mit z. B. Fahrzeugen. Durchbruchsichere Türen, Tore, Schranken oder Poller können helfen, sensible Gebäude oder Anlagen auf dem Gelände zu sichern. Alle Einrichtungen können entweder sehr diskret oder bewusst explizit angelegt werden.

Berechtigte Besucher sind im Rechenzentrum jederzeit willkommen. Der Betreiber muss wissen, wer die Besucher sind und ob sie Infrastruktur- oder Kundenbereiche betreten dürfen. Dies erfordert einen dedizierten und gesicherten Prozess, der berücksichtigt, dass sowohl der Betreiber als auch der Kunde des Rechenzentrums jeweils eigenen Kunden, Dienstleistern und Dritten Zutritt gewähren möchte.

Je nach den Anforderungen des Betreibers und der Kunden können verschiedene Stufen der Sicherheit eingesetzt werden. Der traditionellere Ansatz ist, dass Besucher (und das Personal vor Ort) einen Ausweis besitzen, der ihren Status anzeigt und die richtigen Tore und Türen öffnet. Dieses Verfahren kann jedoch leicht umgangen werden. Moderne Identitätsmanagement-Konzepte verlangen, dass jede Person im Besitz eines Zugangsmediums ist (d. h. eines Ausweises oder eines Smartphones, das z. B. einen QR-Code anzeigt), eine PIN oder ein Passwort kennt und durch Gesichtserkennung, einen Fingerabdruck oder andere Mittel biometrisch identifizierbar ist. Auch die Logistik für Lieferung von Waren muss in das Zugriffsmanagement einbezogen werden. Dabei gewährleistet das System zum einen die korrekte und sichere Lagerung, und zum anderen, die fehlerfreie Zustellung an den berechtigten Empfänger. Das mag kompliziert klingen, doch moderne Technologien automatisieren und vereinfachen viele dieser manuellen Prozessschritte für eine effiziente, kostengünstige und hochwirksame Zutrittskontrolle.

— Technischer Betrieb und Gebäude-management

Rechenzentren haben Tausende von Komponenten, die gesteuert und permanent überwacht werden müssen. Variable Lasten im Rechenzentrum und schwankende Umgebungsbedingungen beeinflussen, welche Parameter für bestmögliche Modalitäten eingestellt werden, um z. B. den Energieverbrauch zu minimieren. Störungen sollten identifiziert werden bevor sie sich auf die Systeme der Kunden auswirken. Die meisten Infrastrukturnetze werden über digitale Systeme ferngesteuert und in ein zentrales Gebäudemanagementsystem (GMS) kaskadiert.

Ähnliche Überlegungen gelten für die Sicherheitssysteme. Die Überwachung des Zustands von Türen, Toren, Schranken und Schleusen ist wichtig, zusammen mit der Verwaltung von Alarmen von Einbruchmeldeanlagen und automatischen Videoüberwachungssystemen sowie der Reaktion auf Alarme von Arbeitsschutzüberwachungs- und Brandmeldesystemen. Dies erfordert eine zentrale Steuerung und Konsolidierung in einem Gefahrenmanagementsystem, um den manuellen Aufwand zu reduzieren.

Um das Rechenzentrum zuverlässig in Betrieb zu halten sind regelmäßige Rundgänge erforderlich, bei denen die orndungsgemäße Funktion aller Betriebs- und Sicherheitssysteme überprüft werden. Außerdem braucht es qualifiziertes, gut geschultes und rund um die Uhr verfügbares Personal aus allen Bereichen wie der Elektrotechnik, Kältetechnik, Sicherheitstechnik und dem Facility Management, um nur einige Funktionen zu nennen.

— Qualitäts- und Prozessmanagement

Kunden erwarten vom Rechenzentrumsbetreiber raffinierte Verfahren zur Prozessgestaltung und -steuerung. Im regulären Betrieb müssen viele Aufgaben auf eine vordefinierte Weise korrekt erledigt werden, die einen unterbrechungsfreien Betrieb garantiert. Einige Beispiele sind:

— Standard Operation Procedures (SOP) und Emergency Operation Procedures (EOP) sind Low-Level-Beschreibungen, wie bestimmte Komponenten während des regulären Betriebs und im Falle möglicher Fehlersituationen zu behandeln sind. Sie müssen für die meisten Aktivitäten im Rechenzentrum jederzeit verfügbar sein.

— Veränderungen der Betriebskomponenten erfordern eine entsprechende Vorbereitung einschließlich Risikoanalyse und Planung von Maßnahmen zur Risikominderung. Der Change-Management-Prozess muss auch die Information der Kunden einschließen, wenn eine Änderung den Betrieb des Kunden beeinträchtigen wird oder könnte.

— Anhand eines effektiven Incident-Management-Prozesses kann zeitnah und planvoll auf Ereignisse im Rechenzentrum reagiert werden. Die Beteiligung der Kunden ist eine Schlüsselkomponente.

— Um über die volle Kontrolle des Betriebs der kritischen Infrastruktur zu verfügen und um unerwünschte Unterbrechungen des Kundenbetriebs zu vermeiden, ist zudem ein zuverlässiges Wartungsmanagement notwendig.

— Das Service Level Management dient dazu, den Kunden über alle Service-Parameter wie Stromverfügbarkeit und -verbrauch, Temperatur- und Luftfeuchtigkeitsprofile, erledigte Serviceanforderungen usw. zu informieren. Die Zusammenfassung der erreichten Service-Levels ist auch intern wichtig als Basis für die Verbesserung der Services, die Leistungsoptimierung, insbesondere im Bereich der Energieeffizienz. Die Messung der Power Utilization Efficiency (PUE) ist entscheidend für die Nachhaltigkeit, aber auch für die finanzielle Situation.

— Das Reklamations- und Beschwerdemanagement muss schnell auf Kundenwünsche oder Kritik reagieren, Lösungen anbieten und an der Kundenzufriedenheit arbeiten.

— Risikomanagement ist ein Schlüsselprozess, sowohl aus interner Sicht, um mögliche technische und administrative Fehlerszenarien zu verstehen, als auch aus Sicht des Kunden. Unternehmen aus regulierten Branchen haben besondere Anforderungen, die Risiken ihrer Geschäftsprozesse zu verstehen. Der Betrieb der IT-Infrastruktur und die Aufrechterhaltung der Verfügbarkeit und Sicherheit der grundlegenden Rechenzentrumsinfrastruktur sind wichtige Bestandteile, bei denen ein Betreiber dieser Dienste in der Lage sein muss, seine Risikoanalysen und die Umsetzung von Maßnahmen zur Risikominderung nachzuweisen.

— Experte für die Anforderungen aus gesetzlichen Vorschriften, Industriestandards und speziellen Kundenbedürfnissen ist das Compliance Managment. Es definiert Verhaltensregeln, veröffentlicht und vermittelt einen Verhaltenskodex und prüft interne Prozesse, um die Einhaltung der festgelegten Regeln sicherzustellen. Viele Unternehmen verlangen darüber hinaus, die Standards in der gesamten Lieferkette einzuhalten. Daraus ergibt sich die Aufgabe, den Verhaltenskodex auch für direkte und indirekte Lieferanten und Dienstleistungspartner zu etablieren.

Prozesse müssen ständig verbessert, dokumentiert und auf dem neuesten Stand gehalten werden. In der Regel ist eine Zertifizierung nach ISO 9001 ein absoluter Mindeststandard, der in vielen Fällen übertroffen werden sollte, um die Kundenerwartungen zu erfüllen.

Tritt ein schwerwiegendes Fehlerereignis ein, das nicht durch das Incident Management abgedeckt werden kann, müssen Business Continuity Management (BCM) Prozesse gestartet werden. Jedes Unternehmen sollte kritische Prozesse mittels einer Business-Impact-Analyse (BIA) untersuchen und Business-Continuity-Pläne für die wichtigsten Ereignisklassen erstellt haben. Um schnell und entschlossen reagieren zu können, muss eine spezielle Organisation definiert und regelmäßig geschult werden, die bei solchen Ereignissen einspringt.

— Business Continuity Management und Katastrophenschutz

Ein fachkundiges, erfahrenes Team überblickt potenzielle Risiken und reagiert unverzüglich auf Katastrophen und Unglücke gemäß eines zuvor entwickleten Business-Continuity- und Katastrophenschutzplans. Je besser Risikoanalysen und -minderung vorab sind, desto unwahrscheinlicher sind solche Situationen. Damit der Plan wirksam und effizient werden kann sind verschiedene Optimierungszyklen notwendig. Unternehmen sollten auf Expertenwissen zurückgreifen, um schnell ein angemessenes Niveau zu erreichen und Fehler zu vermeiden.

— Interne Kontrollen, Vertrauensprinzipien und Berichterstattung

Alle Dienstleister in der IT-Branche stehen vor der Herausforderung, eine Vielzahl von Audits zu beantworten, die von ihren Kunden verlangt werden. Zusätzlich der sonstigen rechtlichen und technischen Standards wollen Kunden sichergehen, dass der Dienstleister bei der Bearbeitung der ihm übertragenen Aufgaben, die aufgestellten Regeln beachtet.

In den vergangenen Jahren wurden Standards entwickelt, mit denen der Dienstleister die Einhaltung dieser Vorschriften nachweisen kann. Diese Standards definieren, wie ein Internes Kontrollsystem (IKS) einzurichten und von einem unabhängigen Wirtschaftsprüfer zu auditieren ist. Ein Testat des Wirtschaftsprüfers über die Einrichtung des IKS und über den Grad der Effektivität und Effizienz wird in einem geprüften Bericht zur Verfügung gestellt.

Die großen Wirtschaftsprüfungsgesellschaften haben sich darauf geeinigt, Berichte zu akzeptieren, die von einer anderen qualifizierten Gesellschaft geprüft wurden, was die Erfüllung der Anforderungen in einem gemeinsamen Ansatz wesentlich erleichtern kann.

Es gibt mehrere Standards für die Einrichtung von Kontrollen, die Prüfung und die Berichterstattung.

— ISAE 3402 definiert Kontrollen, die eingehalten werden müssen, um nachzuweisen, dass die für den Jahresabschluss eines Unternehmens relevanten Systeme zuverlässig betrieben werden und sich, in Bezug auf Rechenzentren, in einer sicheren und verfügbaren Umgebung befinden.

— ISAE 3000 ist ein weiter gefasster Standard, der Prüfungsgrundsätze für Bereiche definiert, die über ISAE 3402 hinausgehen. Ein Auditbericht zur Überprüfung der Einhaltung der Datenschutz-Grundverordnung (DSGVO) könnte unter diesem Prüfungsstandard erstellt werden.

— System and Organization Control (SOC) 1 Reports sind ähnlich wie ISAE 3402, unterliegen jedoch dem SSAE18-Standard, der vom American Institute of Certified Public Accountants (AICPA) erstellt und gepflegt wird. SSAE18 hat sich auch außerhalb der Vereinigten Staaten zu einem Standard entwickelt, da US-Unternehmen den Standard auch international nachfragen.

— System and Organization Control (SOC) 2 Reports, ebenfalls ein Standard der AICPA, konzentrieren sich auf spezielle „Vertrauensbereiche", wie z. B. Kontrollen für Cybersicherheit, Verfügbarkeit, Informationssicherheit oder Datenschutz.

Diese Berichte sind in der Regel entweder als Typ-1-Berichte, bei denen sich der Bericht auf die Vollständigkeit der gesetzten Kontrollen zu einem definierten Zeitpunkt bezieht, oder als Typ-2-Berichte, die den Nachweis der Wirksamkeit über einen Zeitraum von mindestens 6 Monaten erfordern, verfügbar.

Die effektive Implementierung eines IKS kann den Bedarf an Vor-Ort-Audits durch Dritte erheblich reduzieren und hilft zudem, eine verbesserte Managementkontrolle über den Betrieb eines Rechenzentrums zu schaffen.

— Zusammenfassung

Die Entwicklung eines Rechenzentrums erfordert nicht nur Know-how in den Kernbereichen des Geschäftsbetriebs, sondern auch in den Bereichen Regelwerke, Nachhaltigkeit, Zertifizierungen und exzellenter Sicherheit. Eigene Kompetenz in diesen Bereichen ist nicht immer verfügbar, zudem teuer und nicht über den gesamten Lebenszyklus des Rechenzentrums hinweg notwendig. Externe Experten sind unverzichtbar, wenn neue Standorte ausgewählt und für den Betrieb ausgebaut werden. Besonders wertvoll sind Experten, die den gesamten Lebenszyklus eines Rechenzentrums überblicken.

e-shelter security verfügt über mehr als 20 Jahre Erfahrung in der Rechenzentrumsbranche. Kompetente Berater und Ingenieure sowie qualifizierte Partner meistern die Herausforderungen bei der Planung, dem Bau und dem Betrieb eines Rechenzentrums. Mit e-shelter haben sowohl die Betreiber als auch ihre Kunden die Sicherheit, dass ihre Anlagen auf dem neuesten Stand der Rechenzentrumstechnologie sind und der Geschäftsbetrieb optimal und ohne Unterbrechung läuft.

— Wie dürfen wir Sie unterstützen?

T +49 69 247 430 – 000
info@e-shelter.io
e-shelter.io

e-shelter security GmbH
Eschborner Landstr. 100
60489 Frankfurt am Main
T +49 69 247 430 – 000
info@e-shelter.io
e-shelter.io