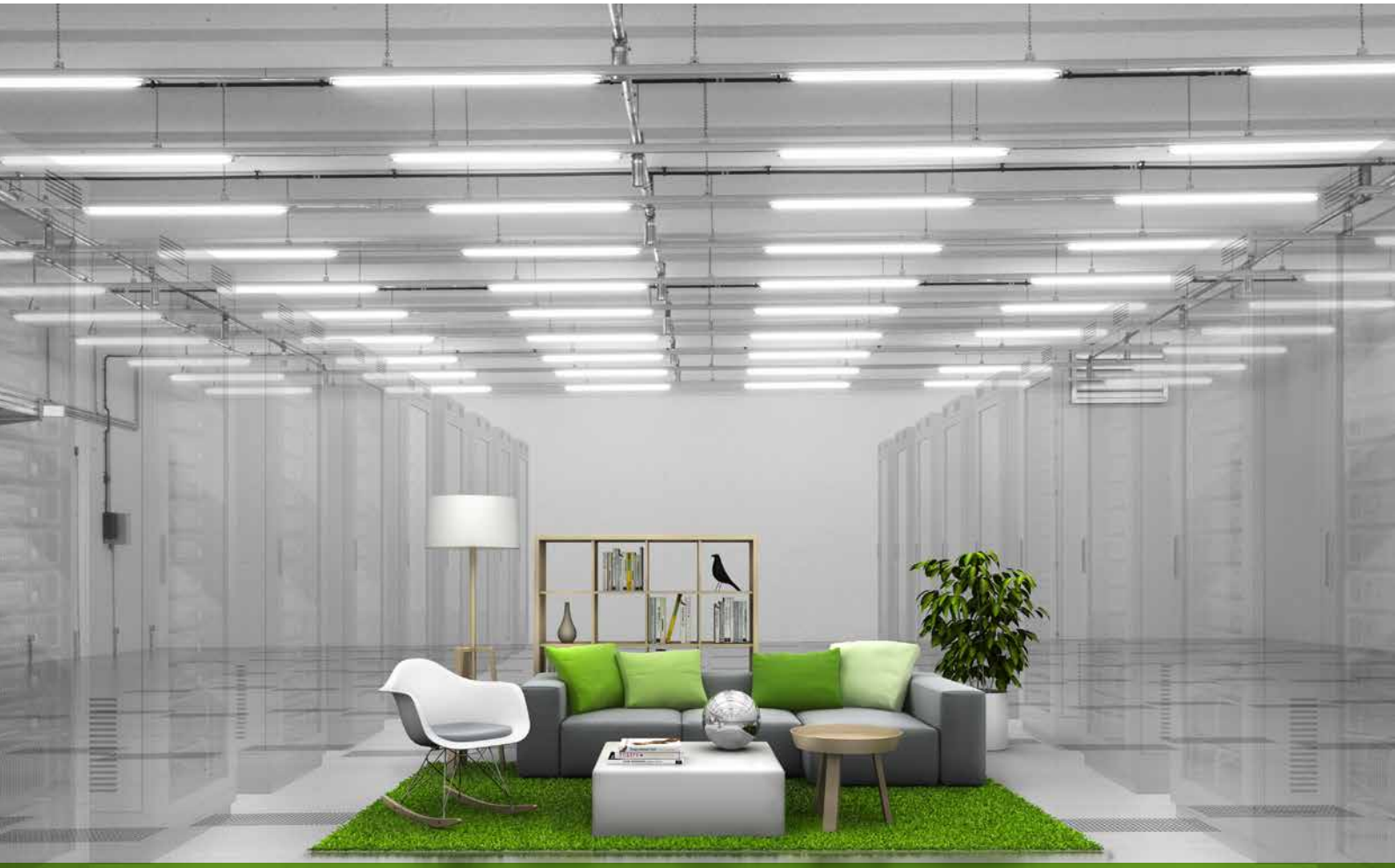
maincubes
SECURE DATACENTERS

WHITEPAPER

Das Datacenter der Zukunft: Die Erfolgsfaktoren der Sicherheit



Ein sicheres Zuhause für Server und Racks

Die Digitalisierung lässt die Datenflut immer weiter anwachsen. Insbesondere Mittelständler sehen sich zunehmend mit Anforderungen konfrontiert, die sie nur mit der Hilfe moderner und professionell gehosteter Rechenzentren (RZ), Stichwort Colocation, erfüllen können. Denn sie müssen darauf vertrauen können, dass ihre IT umfassend und zuverlässig geschützt wird. Dazu sind gleich mehrere tragende Säulen nötig. Welche das sind und wie Anbieter ihre Kunden bei den aktuellen Challenges unterstützen können, zeigt Albrecht Kraas, CTO und einer der Geschäftsführer der maincubes one GmbH, im folgenden Beitrag.

Laut Statista gab es 2017 weltweit rund 8,4 Millionen Rechenzentren jedweder Größe. Kein Wunder, schließlich müssen in einer digitalisierten Welt immer mehr Daten gespeichert, bearbeitet und vorgehalten werden. Als Schmierstoff im Motor einer modernen und digitalen Wirtschaft nehmen sie einen unverzichtbaren Platz ein: Durch multidimensionale Verbindungen zwischen Kunden- und Provider-Services für die verschiedenen Märkte der Zukunft entstehen neue IoT-Eco-Systeme, in denen Rechenzentren die Basis für den Umgang mit Daten bilden. Um dieser Aufgabe gerecht zu werden, müssen sie stets zuverlässig erreichbar und dabei bestmöglich geschützt sein. Kurz: Ein durchgängiges Sicherheitskonzept für ein Datacenter muss kontinuierlich ganz oben auf der Agenda eines Rechenzentrumsbetreibers stehen und folgende fünf Punkte enthalten: Technische Sicherheit, Betriebssicherheit, Datensicherheit im Sinne der ISO 27001, wirtschaftliche Sicherheit und Rechtssicherheit. Zudem sollte als Mindestanforderung die Qualitätsmanagement-Norm ISO 9001 erfüllt werden.

Energiehunger braucht stabile Versorgung

Kein Datacenter kann zuverlässige Arbeit leisten, wenn es immer wieder zu Energieschwankungen kommt. Eine unterbrechungsfreie Stromversorgung (USV) ist demzufolge für jedes Rechenzentrum überlebenswichtig. Dabei kann bereits ein einzelnes so viel Strom verbrauchen wie eine Kommune mit über 10.000 Haushalten. 2016 überholten Frankfurts Rechenzentren sogar Deutschlands größten Flughafen beim Stromverbrauch. Klar ist: Um eine USV bei zugleich hohem Energiebedarf zu jeder Zeit zu garantieren, müssen Anbieter höchste Sicherheitsstandards zwingend einhalten.

Die Nähe zu einem Energieversorger als Primärquelle kann schon ein entscheidender Faktor sein, um eine durchgängige Versorgung sicherzustellen: je kürzer der Leitungsweg, desto geringer der Übertragungsverlust. Denn der ohmsche Widerstand wirkt einerseits generell stärker bei längeren Wegstrecken, andererseits besteht mit jedem weiteren Streckenmeter die Gefahr von Leitungsschäden und damit zusätzlichen Spannungsabfällen. Zudem kann die Zuleitung günstiger redundant erfolgen – möglichst mittels einer 2N-Redundanz –, wenn der Weg zum Stromanbieter sehr kurz ist. Selbstverständlich sollte auch der Energieversorger über modernste Technik und redundante Systeme verfügen. Die Energieversorgung vor Ort ist bei führenden Colocation-Anbietern dann so entworfen, dass in den Serverräumen eine Flächenlast von bis zu zwei Kilowatt pro Quadratmeter und bei Bedarf ergänzende Hotspots von bis zu 20 Kilowatt pro Rack garantiert werden kann.

Falls dennoch alle Stricke der externen Versorgung reißen, muss ein Rechenzentrumsbetreiber eine unterbrechungsfreie Stromanlage vorhalten, die die gesamte Energiezufuhr für mehrere Tage ohne Unterbrechung sicherstellen kann. Ob ein solches Notfallsystem wirklich zuverlässig funktioniert, können nur Tests unter realen Bedingungen klären. maincubes beispielsweise führt regelmäßig sogenannte Black-Building-Tests durch, die die komplette Nutzlast eines Rechenzentrums kombiniert mit diversen Ausfallszenarien bis hin zum Totalausfall der externen Stromversorgung simuliert. Nur Rechenzentren, die solche Härtetests bestehen, können als wirklich zuverlässig gelten.

Cool bleiben im Datacenter

Unzureichende Kühlung kann für IT-Systeme schnell den Hitzetod bedeuten. Immerhin wandeln Milliarden von Transistoren elektrische Energie in Wärme um und müssen daher ununterbrochen gekühlt werden. Ziel ist es, Temperatur und relative Luftfeuchtigkeit in einem Rahmen zu halten, in dem die Technik optimal arbeiten kann. Denn zu hohe Luftfeuchtigkeit lässt Kondenswasser entstehen – und ist die Luftfeuchtigkeit zu niedrig, kann das von statischer Aufladung bis hin zum Kurzschluss führen. Konkret sollte die Temperatur sich zwischen 21 °C und maximal 27 °C bewegen, während die relative Luftfeuchtigkeit im Bereich zwischen 20 und 80 Prozent liegen sollte.

Der Kühleffekt gelingt durch unterschiedliche Maßnahmen: von der Architektur über Passivkühlung mittels Luftaustausch bis hin zur Aktivkühlung mit Kühlmitteln. So kann bereits eine intelligente Fassade zur Abkühlung der Innenräume beitragen. Individuelle Klimaanforderungen in den Serverräumen lassen sich unter anderem durch einzelne und voneinander unabhängige Betriebszonen realisieren. Ein durchgängiges Kaltgangkonzept sorgt für eine physische Trennung von Kühl- und Abluft zwischen den Racks. Der Gesamtaustausch zwischen warmer Innen- und kühlender Außenluft kann über eine moderne Kyoto-Kühlung mit indirekter Freikühlung besonders effizient erfolgen. So gelingt beispielsweise der Betrieb des maincubes

Rechenzentrums in Frankfurt dank des neuartigen Konzepts und Designs komplett ohne zusätzliche Wärmeträger wie Wasser oder Kühlmittel.

Da in der Regel bei den älteren bestehenden deutschen Rechenzentren 80 Prozent der gesamten Stromkosten auf die Kühlung entfallen, müssen Betreiber betriebliche Notwendigkeit und Kosteneffizienz klug abwägen. Der von der Organisation „The Green Grid" ins Leben gerufene PUE-Wert (Power Usage Effectiveness) hilft bei der Einordnung. Er ist der Koeffizient aus dem Stromverbrauch der IT-Komponenten und dem Stromverbrauch aller Nebenaggregate. Demnach wäre ein Idealzustand bei genau 1 erreicht. Während Deutschlands Datacenter im Mittel auf einen PUE-Wert von 1,8 kommen, gilt erst ein Wert von 1,5 als wirklich effizient. Liegt der Wert unter 1,3, handelt es sich um eine sehr effiziente Energienutzung und damit um die Premiumklasse bei Rechenzentren. maincubes bspw. garantiert eine Power Usage Effectiveness unter 1,3 bei einer durchschnittlichen Leistungsdichte.

Ein PUE-Wert unter 1,3 steht für sehr effiziente Energienutzung.

Keine Chance für Brände

Bei aller berechtigten Euphorie rund um die Digitalisierung sind Rechenzentren noch immer Teil der analogen Welt. Sie sind in Gebäuden untergebracht, beheimaten Hardware-Komponenten bestehend aus hunderten Racks, vielen Kilometern Verkabelung und verbrauchen große Mengen an Energie. Demzufolge sind Datacenter auch physischen Gefahren ausgesetzt, vor denen sie bestmöglich geschützt werden müssen. So kann ohne umfangreiche Brandschutzmaßnahmen bereits ein einziger Funke schwerste Schäden verursachen.

Um dieser Gefahr angemessen zu begegnen, ist ein modernes und umfangreiches Brandschutzkonzept unabdingbar. Neben konventionellen Brandmeldesystemen, die sichtbare Rauchentwicklungen registrieren, sollten zusätzlich moderne Anlagen installiert sein, die die Luft kontinuierlich auf kleinste Rauchpartikel überprüfen. Lange vor sichtbarem Rauch lassen sich damit Schwelbrände frühestmöglich erkennen. Kommt es dennoch zum Brand, sind automatische Gaslöschanlagen die erste Wahl. Sie entziehen einem Feuer entweder den Sauerstoff (z. B. durch den Einsatz von Stickstoff oder Argon) oder wirken reaktionshemmend auf den Verbrennungsprozess ein. Die Vorteile: Die eingesetzten Gase haben im Gegensatz zu Löschmitteln wie Schaum oder Wasser keinerlei Auswirkungen auf die Hardware und verflüchtigen sich zudem rückstandslos.

Zutritt nicht gestattet

Rechenzentren zählen wie Kraftwerke zur Kategorie der kritischen Infrastrukturen (KRITIS). Damit sie ihren Dienst zuverlässig leisten, muss der Betreiber auch den Zutritt klar regeln und einschränken. Naheliegend ist demzufolge, das Gelände entsprechend abzuriegeln und bereits für den Außenbereich umfangreiche Videoüberwachung und Bewegungssensoren zu installieren. Der Eintritt in das Gebäude oder in einzelne Abteilungen lässt sich bereits organisatorisch einschränken: So sorgen stabile betriebliche Abläufe dafür, dass befugtes Personal nur in klar vordefinierten Zeiträumen und Umfang Zugang erhält. Gleichzeitig erfolgen mehrstufige Zutrittskontrollen über Sicherheitsschleusen. Personen sollten sich hier mittels Biometrie authentifizieren müssen. Besonders dafür geeignet sind etwa moderne Handvenen-Scanner, die mittlerweile sicherer und zudem benutzerfreundlicher als Iris-Scanner sind. Außerdem kontrollieren sowie regulieren Vereinzelungsanlagen Zugänge unter höchsten Sicherheitsanforderungen.

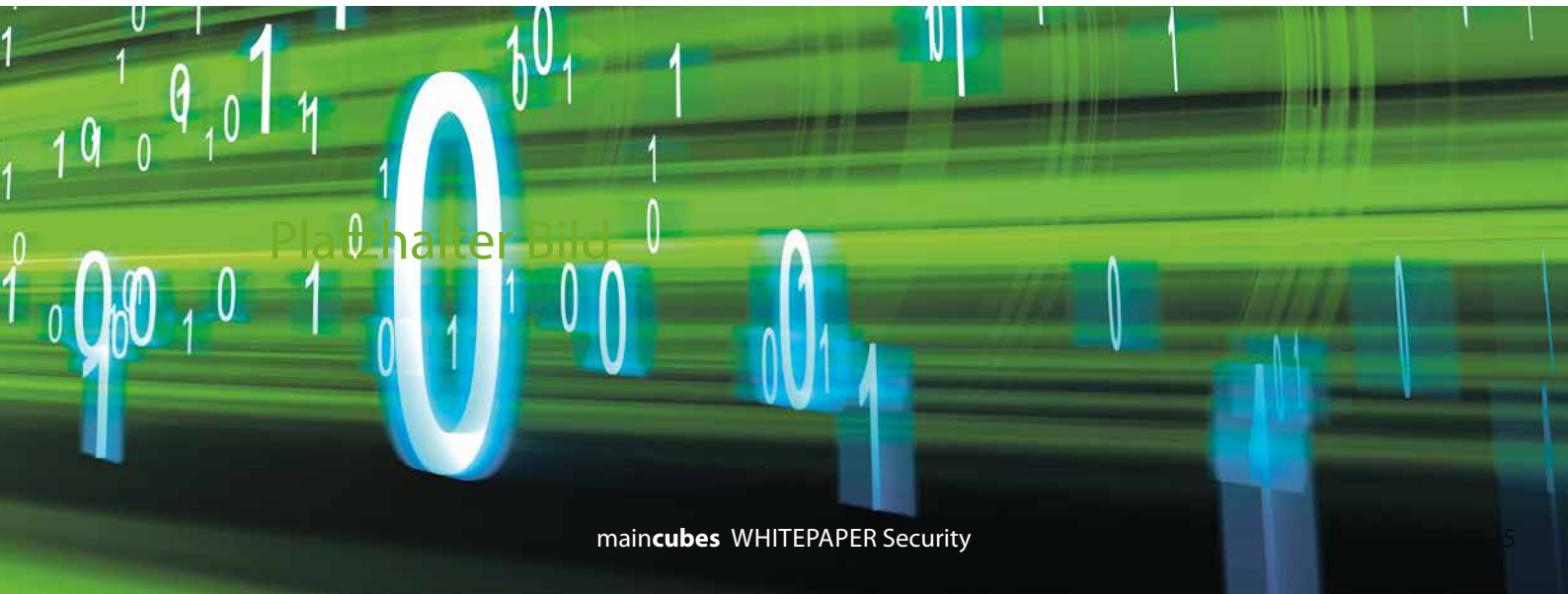
Auch im Gebäudeinneren helfen umfangreiche Videoüberwachung und empfindliche Bewegungssensoren dabei, Personen sofort zu registrieren und ihren Aufenthaltsort zu dokumentieren. Zudem muss ein modernes Datacenter über einen 24-Stunden-Sicherheitsdienst verfügen, der im Notfall jederzeit eingreifen kann. So ergänzt die menschliche Komponente auf sinnvolle Weise die technischen Maßnahmen und sorgt für ein redundantes Security-Konzept für die gesamte Anlage.

Standort ist entscheidend

Moderne Datenübertragungstechnik stellt immer wieder neue Rekorde auf. Demzufolge gehen viele davon aus, dass es eigentlich keine Rolle spiele, wo genau ein Rechenzentrum steht. Doch das ist ein Irrtum. Der Standort ist auf verschiedenen Ebenen ein ganz entscheidender Faktor beim Thema Security: von der geographischen Lage über die rechtsstaatliche Verfassung bis hin zur Infrastruktur.

Die Grenzen der Natur akzeptieren

Umwelteinflüsse können etwa darüber entscheiden, wie sicher der Standort eines Rechenzentrums ist. Risikofaktoren wie schwere Unwetter, Erdbeben, Überschwemmungen oder extreme Hitze treiben die Kosten stark in die Höhe oder machen den Betrieb gar vollständig unmöglich. Daher kommen geographisch nur möglichst sichere Regionen für den Standort eines Datacenters in Frage. Zudem sollten auch die klimatischen Bedingungen nicht unterschätzt werden: Ein moderates Klima, wie man es etwa in Deutschland vorfindet, erlaubt beispielsweise unter Einsatz moderner Technologie eine Zukühlung von höchstens 20 Prozent. Das senkt neben dem Energieverbrauch auch die Kosten und ist darüber hinaus umweltschonender.



Politische Rahmenbedingungen

Auch die politische/rechtsstaatliche Verfassung übt einen großen Einfluss auf die Sicherheit eines Rechenzentrums aus. Grundsätzlich sorgen zum Beispiel stabile politische Verhältnisse für mittel- und langfristige Investitionssicherheit. Eine freiheitlich demokratische Staatsordnung mit Gewaltenteilung und konstitutionell zugesicherten Rechten zur Vertragsfreiheit sowie dem Schutz der informationellen Selbstbestimmung des Einzelnen bilden einen starken Rahmen für ein hohes Maß an Sicherheit von Daten. Bindende Rechtsvorschriften wie etwa das Bundesdatenschutzgesetz (BDSG) zusammen mit der Datenschutz-Grundverordnung (DSGVO) und dem IT-Sicherheitsgesetz bescheinigen beispielsweise dem Standort Deutschland besondere Kompetenzen in Sachen Datenschutz und -sicherheit. So glänzt die Bundesrepublik heute weltweit mit dem Slogan „Security made in Germany" und sorgt dafür, dass Betreiber von Datacentern ihre Sicherheitskonzepte noch umfangreicher gestalten. Zugleich ist auch die nationalstaatliche Zugehörigkeit wichtig: Während etwa US-Provider sich in einer Zwickmühle zwischen europäischem und amerikanischem Recht befinden, gelten in Deutschland für deutsche Betreiber nur die Rechtsvorschriften der Bundesrepublik bzw. der Europäischen Union.

Hohe Sicherheitsvorschriften, technische Standards sowie Kontrollinstanzen mit weitreichenden Befugnissen bieten einen zusätzlichen formellen Rahmen. Internationale Normen für das Qualitätsmanagement wie die ISO 9001 oder die ISO 27001 im Bereich des IT-Sicherheitsmanagements bieten Orientierung und klare Vorgaben. Kontrollbehörden oder private Prüforganisationen wie der TÜV in Deutschland können etwa durch Zertifikate die geprüfte Sicherheit sowie Zuverlässigkeit bescheinigen. Auch für die DSGVO wird derzeit an einem Zertifikat gearbeitet, das sich am noch gültigen TCDP (Trusted Cloud Datenschutz-Profil) orientiert.

Infrastruktur auf mehreren Ebenen

Zuletzt ist auch die Infrastruktur auf verschiedenen Ebenen ein wichtiger Faktor im Sinne von Energie, Transportwegen, dem Zugang zu modernen Datenübertragungstechnologien und Bildung. So sorgt etwa der direkte Zugang zu großen Internetknoten wie dem DE-CIX in Frankfurt für die sichere Anbindung an die weltweiten Datenströme. Selbst die Mentalität gegenüber Technik innerhalb einer Gesellschaft kann sich positiv oder negativ auf die Standortsicherheit eines Rechenzentrums auswirken.

Entweder ganz oder gar nicht

Das Konzept der physischen Sicherheit eines Rechenzentrums ist, wie bei einer Kette, nur so stark wie ihr schwächstes Glied. Nur eine sorgfältig austarierte, ISO-zertifizierte Gesamtstrategie sorgt dafür, dass beispielsweise Colocation-Kunden sich voll und ganz auf ihren Anbieter verlassen können. Allein bei der Frage der Ausfallsicherheit sollten nur Betreiber in Frage kommen, die mindestens das TÜV Level 3 erreichen, was analog zum Tier 3-Standard ist, und somit eine 99,98-prozentige Verfügbarkeit gewährleisten können.

Moderne Konzepte zeigen, dass Sicherheit, Kosteneffizienz und Umweltschutz sich problemlos in Einklang miteinander bringen lassen. Das beweisen auch immer wieder die Preisträger des seit 2011 verliehenen Deutschen Rechenzentrumspreises mit ihren hochinnovativen Ideen. Die Herausforderungen etwa der Industrie 4.0 oder des IoT unter der Ägide der Digitalisierung machen neue Denkansätze und Konzepte zwingend notwendig, wie beispielsweise die secure**exchange**-Plattform von maincubes. Sie bietet neben umfangreichen Sicherheitspaketen auch eine direkte Vernetzung von Marktpartnern, die dort ihre eigenen Services anbieten, Informationen austauschen, neue Features in die Angebote integrieren und flexibel in neue Bereiche wie Digital Factory, Secure Mobility, Smart City oder Secure Payment einsteigen können. Es entsteht ein Eco-System, das in der digitalen Ära zunehmend erfolgsentscheidend ist. Denn an einer gemeinsamen Nutzung von Ressourcen in einem Netzwerk wird künftig kein Unternehmen mehr vorbeikommen, da die umfassenden Herausforderungen alleine kaum mehr zu erfüllen sind. Die horizontale Vernetzung auf einem sicheren „Marktplatz der Digitalisierung" weist daher den Weg in die Zukunft.

Autor: Albrecht Kraas, CTO und einer der Geschäftsführer der maincubes one GmbH

Stand: Oktober 2018

maincubes
SECURE DATACENTERS

maincubes.com

maincubes one GmbH Frankfurt am Main +49 69 6976810-20 info-de@maincubes.com