CLOUD
& MANAGED SERVICES

2023
CHF 20.–

Market | Infrastructure | Operations | XaaS

So kommen Unternehmen sicher in die Cloud

Partner

EuroCloud SWISS | SWICO

Ihre Daten sind Gold wert.

Wenn es um IT und Verfügbarkeit geht, spricht alles dafür, bestehende Inhouse-Lösungen zu Green auszulagern.

Die Green Datacenter sind versorgungssicher, technologisch jederzeit auf neustem Stand und nach aktuellen Kriterien der Nachhaltigkeit und Energieeffizienz konzipiert. Das Angebot umfasst alles vom Einzelrack über Cages und Suiten oder Raum für Hyperscaler bis zum Green Ecosystem für massgeschneiderte Cloud-Lösungen.

green

Wie immer Sie Ihre IT-Zukunft gestalten und sichern möchten, wir garantieren Ihnen:

All you need is Green.

www.green.ch

Cloud stösst auf Gegenwind

Das bisschen Kritik, das den Cloud-Fürsprechern gelegentlich um die Ohren fliegt, dürfte dem Geschäft kaum schaden.

Joël Orizet,
leitender Redaktor, Netzwoche

Jede Technologie hat ihre Schattenseiten. Das geht allerdings schnell vergessen, wenn man sich nach Meinungen über Cloud Computing umhört. Denn nahezu unisono heisst es, die Cloud biete gegenüber dem Betrieb einer eigenen IT-Infrastruktur ein ganzes Füllhorn an Vorteilen. Zum Beispiel: flexible Betriebskosten statt starre Kapitalkosten; Skalierbarkeit auf Knopfdruck statt Hardware-Beschaffungen auf Vorrat; geteilte statt alleinige Verantwortung für die Datensicherheit. Abseits aller Lobeshymnen sind jedoch auch kritische Stimmen zu hören. Neulich zum Beispiel in der «Financial Times».

Cloud Computing macht abhängig – und die Abhängigkeit der Unternehmen von nur wenigen Cloud-Providern ist ein Problem, wie die britische Tageszeitung berichtet. Die Cloud-Migration setze Unternehmen einem erhöhten Risiko von Cyberangriffen sowie Datenschutzverletzungen aus. Und somit auch der Gefahr von Geldstrafen und Reputationsschäden. Das Problem geht dem Bericht zufolge sogar weit über betriebswirtschaftliche Risiken hinaus. Die zunehmende Abhängigkeit des Finanzsektors von Cloud-Diensten führe dazu, dass die Technologie zum «Single Point of Failure» werde. Demnach könnte ein Ausfall der Cloud schlimmstenfalls zu einem Ausfall des Finanzsystems führen, weil die meisten Banken und Versicherer auf denselben Cloud-Provider setzen.

Dagegen liesse sich einwenden, dass man dieses Risiko reduzieren kann, indem man nicht nur auf einen, sondern auf zwei oder drei Cloud-Anbieter setzt. Einige Branchenexperten zeigen sich jedoch skeptisch, was die vermeintlichen Vorteile einer solchen Multi-Cloud-Strategie angeht. Der Ansatz mache den Grossteil der Argumente für die Nutzung der Cloud zunichte, sagte Gartner-Analystin Lydia Leong gegenüber der «Financial Times». Denn: Multi-Cloud sei komplex und kostspielig. Auch wer nur eine Cloud nutzt, spart damit nicht zwangsläufig Geld. Das Mieten von Computern sei für KMUs mit stabilem Wachstum meistens sogar ein schlechtes Geschäft, schreibt David Heinemeier Hansson, CTO und Mitgründer der Softwarefirma Basecamp sowie Schöpfer des Webframeworks Ruby on Rails, in einem Blogbeitrag, in dem er ausführt, warum sich sein Unternehmen aus der Cloud zurückzieht. Für den Rückzug aus der Cloud gibt es sogar einen Begriff: Cloud Repatriation.

Ob die damit gemeinte Rückführung von Applikationen von einer Public Cloud in eine Private Cloud oder in ein hauseigenes Rechenzentrum tatsächlich ein Trend ist, darf man jedoch bezweifeln. Verlässliche Zahlen dazu gibt es nicht. Und der gesunde Menschenverstand spricht eher dagegen. Denn wer sich erst einmal an die Annehmlichkeiten gewöhnt hat, die Cloud-Dienste zweifellos bieten, braucht gute Gründe, um darauf zu verzichten.

Kann sein, dass sich manche IT-Firmen austoben wollen und Freude daran haben, eigene Infrastrukturen aufzubauen und zu unterhalten – rechnen dürfte sich das aber, wenn überhaupt, nur in wenigen Fällen. Gut möglich ist hingegen, dass einige Unternehmerinnen und Unternehmer schlechte Erfahrungen mit dem sogenannten Vendor-Lock-in gemacht haben, dass also die Abhängigkeit von den Plattformen der Hyperscaler für sie zum Problem geworden ist. In solchen Fällen spricht jedoch nur wenig gegen die Cloud an sich, sondern vieles für Open-Source-Software. Das versprechen zumindest die Verfechter quelloffener Systeme.

Hört man den Anbietern, den Analysten, ja sogar dem Bundesrat zu, tönt es einstimmig: Die Cloud ist ein probates Mittel, um digitale Dienste möglichst schnell und effizient umzusetzen. Folglich landen mehr und mehr Ressourcen zur Datenverarbeitung über kurz oder lang in der Cloud – Ausnahmen für besonders schützenswerte Daten vorbehalten. Ob man das nun gut findet oder nicht, spielt keine Rolle. Wichtig ist nur, dass man es richtig anstellt. Was wiederum bedingt, dass sich die Anbieter wie auch die Verbraucher und vor allem die Regierungen ernsthaft mit den Schattenseiten auseinandersetzen, sei es bezüglich Datenschutz, Patzern beim Beschaffungsprozess oder bezüglich der Risiken von Abhängigkeiten. Das bisschen Kritik, das den Cloud-Fürsprechern gelegentlich um die Ohren fliegt, dürfte dem Geschäft kaum schaden. Vielleicht sogar im Gegenteil, weil gelegentliche Kritik die Glaubwürdigkeit erhöht. Vielleicht läuft es im Cloud-Business ja ähnlich wie beim Flugzeug fliegen: Gegenwind erhöht den Auftrieb.

IMPRESSUM

Verlag
Netzmedien AG / Heinrichstrasse 235 /
CH-8005 Zürich / Tel. +41 44 355 63 63
Redaktion: desk@netzmedien.ch
Verlag: info@netzmedien.ch
Anzeigen: inserate@netzmedien.ch
Aboservice: abo@netzmedien.ch
Druck: Werner Druck Basel gedruckt in der schweiz

Erscheinungsweise
Eine Publikation der Reihe «IT for ...»
Erscheint als Eigenbeilage zu «Netzwoche» und «IT-Markt»
Einzelausgabe (Schweiz): CHF 20.–
Auflage: 15 600 Ex.

Partnerplattformen
netzwoche www.netzwoche.ch
IT-MARKT www.it-markt.ch
ICTjournal ict-journal.ch

Sie erreichen alle Mitarbeiter telefonisch unter
+41 44 355 63 + jeweilige Endziffern oder per
E-Mail: vorname.nachname@netzmedien.ch

CEO & Verleger: Dr. Heinrich Meyer (+31)
Projektleitung Awards, Assistentin des CEO: Seraina Frehner (+35)
Head of Sales: Markus Stotz (+34)
Sales: Colette Mader (+39)
Sales Consultant: Konstantinos Georgiou (+33)
Sales W-CH: Supannika Chavanne
Sales-Support: Patrizia Zbinden (+69)
Praktikant Sales: Sascha Augstburger (+63)
Buchhaltung: Christina Frischknecht (+30)
Grafik/Layout: Samantha Maurer (+65)
Grafik/Layout: Galledia AG
Junior Media Manager: Reto Suter (+32)

Redaktion
Marc Landis (mla), Chefredaktor (+36)
Joël Orizet (jor), leitender Redaktor (+68)
Leslie Haeny (lha), stv. Chefred. CEtoday (+66)
Coen Kaat (cka), stv. Chefred. IT-Markt (+64)
Susanne Löbe, CvD/Korrektorat/Layout (+61)
Kevin Fischer (kfi), Redaktor
René Jaun (rja), Redaktor (+68)
Tanja Mettauer (tme), Redaktorin (+60)
Maximilian Schenner (msc), Redaktor (+38)
Yannick Züllig (yzu), Redaktor (+68)
Adrian Oberer (aob), Praktikant (+64)
Pascal Wojnarski (pwo), Praktikant

Redaktion Westschweiz
Rodolphe Koller (rko), Yannick Chavanne (ych)

Abraxas gründet Sparte fürs Cloud-Geschäft

Den vollständigen Artikel finden Sie online
www.netzwoche.ch

rja. Der Ostschweizer IT-Dienstleister Abraxas gründet eine neue Geschäftseinheit. Mit der neuen Abteilung Public Cloud Services wolle man Städte und Kantone dabei unterstützen, die eigene IT-Infrastruktur cloud-ready weiterzuentwickeln, leistungsfähige Cloud-Umgebungen zu nutzen und modernes Arbeiten aus der Cloud einzuführen, teilt der St. Galler IT-Dienstleister mit.

Der designierte Leiter des neuen Geschäftsbereichs ist Dieter Gasser. Er tritt die Stelle per Anfang Januar 2023 an. Bis dahin fungiert Gasser noch als COO von Itnetx, einem Microsoft-Cloud-Spezialisten, wie Abraxas schreibt. Itnetx gehört seit 2019 der Swisscom.

Laut der Mitteilung verfügt Gasser über rund 25 Jahre Erfahrung in der IT-Branche. Zuerst Applikations-, Web- und Datenbankentwickler gründete er 2011 den IT-Dienstleister Syliance im Bereich Microsoft Systems Management. Seine fachlichen Schwerpunkte liegen laut Mitteilung auf IT-Service-Management, Prozessautomatisierung, Big Data, IT-Strategie und insbesondere Cloud-Adoption.

Zuger Cloud-Dienstleister geht in deutsche Hände

Den vollständigen Artikel finden Sie online
www.netzwoche.ch

aob. Der Zuger Cloud-Dienstleister Miracle Mill hat einen neuen Besitzer. Das deutsche Investment-Unternehmen Nord Holding übernahm die Firma mit Sitz in Baar und integrierte sie in die hauseigene Public Cloud Group (PCG). Durch die Akquisition ergänzt PCG sein Serviceangebot im Bereich der Cloud-nativen Applikations- und Softwareentwicklung, wie Nord Holding mitteilt. Ausserdem trete die PCG durch den Zukauf von Miracle Mill in den Schweizer und den schwedischen Markt ein.

Zu den finanziellen Details der Übernahme machen die Unternehmen keine Angaben. Miracle Mill beschäftigt gemäss Mitteilung rund 100 Mitarbeitende. In den kommenden Jahren wolle man die Belegschaft verdoppeln, heisst es weiter.

Mit Teams an zusätzlichen Standorten in Nordmazedonien und Bulgarien bilde Miracle Mill den Development-Hub der PCG und solle so das Wachstum der Gruppe unterstützen. Mit der Akquisition sei die PCG dem Ziel eines vollumfänglichen Multi-Public-Cloud-Service-Portfolios einen Schritt näher gekommen.

Neuer Leitfaden für die Nutzung externer Cloud-Dienste in Zürich

Dominika Blonski, Datenschutzbeauftragte des Kantons Zürich.
Bild: datenschutz.ch

kfi. Dominika Blonski, seit Mai 2020 Datenschutzbeauftragte des Kantons Zürich, hat einen neuen Leitfaden für die Nutzung externer Cloud-Dienste herausgegeben. Er richtet sich an Mitarbeitende öffentlicher Organe, die Cloud-Dienste evaluieren.

Im Text heisst es, dass das öffentliche Organ bei der Bearbeitung von Daten in externen Cloud-Diensten dieselbe Verantwortung trage, wie wenn es die Informationen selbst bearbeiten würde. Damit sei es auch für die Auswahl, Instruktion und Überwachung des Cloud-Anbieters verantwortlich. Cloud-Dienste müssten die Grundrechte der betroffenen Personen gleichwertig schützen, wie es das öffentliche Organ bei der Datenbearbeitung selbst tue.

Den vollständigen Artikel finden Sie online
www.netzwoche.ch

Evaluation und Folgenabschätzung

Verantwortliche der öffentlichen Organe müssten evaluieren, ob gesetzliche Bestimmungen wie Geheimhaltungsvorschriften oder vertragliche Vereinbarungen eine Auslagerung in die Cloud erlaubten. Dabei betont die Datenschutzbeauftragte einen Punkt: «Werden Personendaten oder besondere Personendaten bearbeitet und kann für die vorgesehene Cloud-Lösung weder schweizerisches Recht noch ein schweizerischer Gerichtsstand vereinbart werden, ist die Auslagerung nicht datenschutzkonform.» Dies gelte auch für den Fall, dass der Auftragnehmer keine Möglichkeit der Datenverschlüsselung anbiete. «In diesen Fällen kann die vorgesehene Cloud-Lösung nicht eingesetzt werden.»

Ausgaben für Cloud-Sicherheit steigen

Den vollständigen Artikel finden Sie online
www.netzwoche.ch

ych/rja. Eine Cloud-Umgebung abzusichern, geht ins Geld. Laut den aktuellen Zahlen des Marktforschers Gartner macht Cloud-Sicherheit den grössten Anteil der Kosten aus, die Unternehmen insgesamt in Cybersicherheit investieren. An zweiter Stelle folgen demnach Ausgaben für den Schutz von Applikationen. Gartner nennt drei Faktoren, welche die Ausgaben für IT-Sicherheit in die Höhe treiben: die zunehmende Verbreitung von Remote- und Hybrid-Arbeit, den Übergang von VPNs zu Zero-Trust-Network-Access-Modellen (ZTNA) und schliesslich die generelle Migration vieler Unternehmen in die Cloud.

«Die Pandemie hat das hybride Arbeiten und den Wechsel zur Cloud beschleunigt und CISOs vor die Herausforderung gestellt, ein zunehmend verteiltes Unternehmen zu sichern», fasst Gartner-Analyst Ruggero Contu zusammen.

2023 sollen die Ausgaben um 26 Prozent steigen

Konkret prognostiziert Gartner, dass im Jahr 2022 die Ausgaben für Cloud-Sicherheit um 22 Prozent, und im Jahr 2023 um 26 Prozent ansteigen werden. Das ist weniger als im Jahr 2021, als die Kosten um 36 Prozent in die Höhe schnellten. Die Ausgaben betreffen laut dem Marktforscher vor allem die beiden Segmente Cloud Access Security Broker (CASB) und Plattformen für den Schutz von Cloud-Workloads (Cloud Workload Protection Platforms, CWPP). Auch in cloudbasierte IT-Sicherheitstools werde in den nächsten Jahren verstärkt investiert.

Laut einer anderen Gartner-Untersuchung vom September 2022 streben drei Viertel der Firmen eine Konsolidierung ihrer Security-Anbieter an. Allerdings will nur eine Minderheit so Kosten sparen; die meisten Firmen vereinheitlichen aus anderen Gründen, namentlich aufgrund von Zeitmangel und wegen zu starrer Zulieferpartnerschaften.

Bild: Asierromero / Freepik.com

Amazon und Google kritisieren Microsofts Cloud-Strategie

yzu. Per 1. Oktober 2022 hat Microsoft seine Richtlinien bezüglich Cloud-Lizenzierung überarbeitet. Dadurch soll es künftig einfacher werden, Microsoft-Dienste wie etwa Windows Server auf einer Nicht-Microsoft-Cloud zu hosten. Das würde es Cloud-Service-Anbietern erleichtern, miteinander zu konkurrieren.

Diese Änderungen stossen jedoch den anderen grossen Cloud-Providern Google, AWS und Alibaba sauer auf, wie «Reuters» berichtet. Denn die drei Hyperscaler sind explizit von den neuen Lizenzierungsbedingungen ausgenommen. Wer also Microsoft-Dienste auf einer AWS- oder Google-Cloud nutzen will, sieht sich mit höheren Kosten und diffusen Regulierungen konfrontiert.

Vorwurf der Wettbewerbseinschränkung

Microsofts neue Richtlinien würden den Wettbewerb auf unfaire Weise verzerren, sagte ein Sprecher von AWS gegenüber «Reuters» und ergänzte: Mit den Änderungen sorge Microsoft für noch mehr Beschränkungen, «statt auf seine Kunden zu hören und eine faire Softwarelizenzierung in der Cloud für alle wiederherzustellen».

Den vollständigen Artikel finden Sie online
www.netzwoche.ch

Google äussert seine Kritik ebenfalls öffentlich: In einem Twitter-Thread schreibt Marcus Jadotte, Vice President Government Affairs & Policy bei Google Cloud, dass man an alle Cloud-Provider appelliere, ihre Kunden nicht vertraglich an sich zu binden und stattdessen mit den Stärken ihrer Technologien zu konkurrieren. «Das Versprechen der Cloud ist flexibles, elastisches Computing ohne vertragliche Bindung. Kunden sollten in der Lage sein, sich frei zwischen den Plattformen zu bewegen und die Technologie zu wählen, die für sie am besten funktioniert, und nicht die, die am besten für Microsoft funktioniert», twitterte Jadotte.

Strommangellage – ist Auslagerung in die Cloud die Lösung?

Was passiert, wenn Ihr Server plötzlich keinen Strom mehr erhält? Auch wenn es keine Garantien bezüglich Stromverfügbarkeit gibt, das Datacenter ist der bestmögliche Ort, an dem sich Ihre Server und Workloads befinden können. Aber für welche Art von IT-Outsourcing soll man sich entscheiden?

Die Autorin
Karin Würzberger,
Marketing Manager,
Cyberlink

Die Herausforderungen durch die aktuelle geopolitische Lage sprechen eindeutig für die IT-Auslagerung, denn mit der Absicherung und Resilienz eines Tier-3-Datacenters können Unternehmensstandorte kaum mithalten. Datacenter verfügen nicht nur über eigene Notstromaggregate, um kurzfristige Stromausfälle zu überbrücken. Bei einer Strommangellage zählen sie aller Wahrscheinlichkeit nach auch zu den kritischen Infrastrukturen, die von Kontingentierungen des Bundes ausgenommen sind.

Colocation oder Cloud?

Unternehmen, die auf die eigene IT-Infrastruktur nicht verzichten wollen, diese aber nicht mehr vor Ort betreiben möchten, entscheiden sich für Colocation. Die Stromversorgung ist im Datacenter bestmöglich gesichert und die Server bleiben in der Verantwortung des Unternehmens. Wenn doch eher eine Cloud-Lösung in Betracht gezogen wird, ist die Stromversorgung im Datacenter ebenfalls gesichert, aber Hardware und IT-Infrastruktur werden gestellt. Cloud-Services bieten zusätzlich grösstmögliche Flexibilität, um Leistungsparameter auch kurzfristig nach oben oder auch nach unten anpassen zu können. Zudem sind Redundanz-Lösungen deutlich günstiger als im Colocation-Bereich realisierbar. Für Unentschlossene bietet Cyberlink mit Disaster Recovery as a Service (DRaaS) einen cloudbasierten Service, der Daten, Applikationen und IT-Infrastruktur gleichermassen absichert, ohne gleich den produktiven Betrieb in die Cloud auszulagern. Die Datenverarbeitung wird nur im Desaster-Fall in die Cloud verlagert und Mitarbeitende können bei einem Stromausfall im Büro vom Homeoffice aus weiterarbeiten. Auslagerung ja, aber ob Colocation, Cloud oder erst einmal mit DRaaS beginnen, unsere Experten unterstützen Sie bei der Entscheidungsfindung, welche Option zu Ihrem Unternehmen passt.

Sicher und begleitet in die eigene Cloud.

Cyberlink lässt Sie nicht allein. Mit einem exklusiven Onboarding-Workshop unterstützen unsere Cloud Engineers Sie beim Einrichten der Cloud-Lösung inklusive Konfiguration und Test unter Beachtung aller Spezifikationen. Im Rahmen eines Proof of Concept (PoC) kann eine auf Ihre Bedürfnisse abgestimmte Cloud-Lösung drei Monate lang getestet werden. Mit diesem kostenlosen und jederzeit kündbaren Service können Cyberlink-Kunden den Leistungsumfang vorab prüfen und sich selbst ein Bild davon machen, welche operativen und finanziellen Vorteile ihnen zusätzlich durch die skalierbare Lösung sowie die nutzungsbasierte Abrechnung bei vollständiger Kostentransparenz entstehen.

Die Strompreisentwicklung wird jeden treffen.

Die jüngsten globalen Ereignisse werden in allen Bereichen zu einer deutlichen Kostensteigerung für den Energiebezug führen. Diese müssen insbesondere im Falle einer Colocation-Lösung auf den Kunden abgewälzt werden. Um diesen Umstand abzumildern, unterstützen wir schon heute unsere Kunden bei allfälligen Sparmassnahmen, die durch einen optimierten Server-Einsatz, das temporäre ausser Betrieb setzen oder gar durch die Auslagerung in die Cloud Energiekosten senken können. Daneben sind die Datacenter-Betreiber selbst laufend um die weitere Steigerung der Energieeffizienz bemüht.

Eine der modernsten Cloud-Plattformen der Schweiz bietet Sicherheit.

Die Virtual Private Cloud (VPC) von Cyberlink wird ausschliesslich in hochsicheren Tier-3-Rechenzentren im Raum Zürich betrieben, bietet modernste Infrastructure as a Service (IaaS) und wird regelmässig von einem unabhängigen Auditor nach ISAE-3402 überprüft. Die Datacenter-Infrastrukturen genügen strengsten Sicherheitsanforderungen wie jenen der Eidgenössischen Finanzmarktaufsicht (FINMA).

KEY FACTS

- Bestmögliche Stromversorgung
- Datenhaltung & Betrieb in der Schweiz
- Hochsichere Tier-3-Datacenter
- Flexible Dimensionierung
- Persönlicher Service

Colocation

- Dynamisch skalierbare Leistungsparameter
- 7/24h Zugang zu Ihrer Infrastruktur
- Zertifizierte Sicherheit & Effizienz

Cloud

- Modernste Cloud-Architektur (powered by VMware)
- Kostengünstige Redundanz-Lösungen
- Attestierte Qualität (ISAE 3402)
- Nutzungsbasierte Abrechnung
- Gratis Proof of Concept (PoC) für VPC & DRaaS
- Onboarding-Workshop

cyberlink

Kontakt

Daniel Hildinger.
Key Account Manager
sales@cyberlink.ch

Das Vantage-Rechenzentrum in Winterthur ist einer von drei AWS-Standorten in der Schweiz. Bild: vantage-dc.com

Amazon Web Services eröffnet Schweizer Cloud-Region

Amazon Web Services eröffnet in Zürich seine Schweizer Infrastruktur-Region. Damit können Kundinnen und Kunden ihre Anwendungen und Daten auf Servern in der Schweiz unterhalten. Das Unternehmen plant bereits weitere Investitionen in der Schweiz. Autor: Adrian Oberer

Vor zwei Jahren hat Amazon Web Services (AWS) die Eröffnung eines Schweizer Cloud-Standorts angekündigt. Nun liess die Amazon-Tochter den Worten Taten folgen und eröffnete in Zürich seine erste Schweizer Infrastruktur-Region, wie das Unternehmen mitteilt. Damit biete AWS seiner Schweizer Kundschaft eine hohe Verfügbarkeit bei niedriger Latenz von Servern im Inland.

Die neue «AWS Europe (Zürich) Region» ist erst die siebte Cloud-Region des Hyperscalers in Europa und besteht aus drei sogenannten Availability Zones, wie AWS weiter schreibt. Dabei handle es sich um geografisch und damit physisch getrennte Teile der Infrastruktur, die durch redundante Netzwerke untereinander verbunden werden. Die verschiedenen Zonen verfügen gemäss Mitteilung über eine unabhängige Stromversorgung, Kühlung und physische Absicherung. Trotzdem lägen sie nahe genug beieinander, um «extrem niedrige» Latenzzeiten zu ermöglichen. Dadurch unterstütze die Infrastruktur auch Hochverfügbarkeitsanwendungen.

Auch mehrere Verfügbarkeitszonen möglich

Die Schweizer Kundschaft kann nun also die eigenen Anwendungen auf Servern in der Schweiz anbieten. Um die Fehlertoleranz und damit die Verfügbarkeit der eigenen Anwendung zu verbessern, können Kundinnen und Kunden ihre Anwendungen auch so konzipieren, dass diese in mehreren Availability Zones gleichzeitig laufen, wie AWS mitteilt. Zusätzlich ermögliche es die Einführung der Schweizer AWS-Region der lokalen Kundschaft mit Anforderungen an die Datenresidenz, ihre Daten sicher in der Schweiz zu speichern.

Offiziell macht AWS keine Angaben zum genauen Standort oder der Betreiberfirma seiner Schweizer Rechenzentren. Gemäss «Inside-IT» mietete sich das Unternehmen aber an den Standorten Lupfig, Winterthur und Glattbrugg bei den RZ-Betreibern Green, Vantage und Interxion ein. Dies hätten mehrere mit der Branche vertraute Expertinnen und Experten unabhängig voneinander bestätigt.

Weitere Investitionen geplant

Für die kommenden Jahre plant AWS weitere Investitionen in der Schweiz, wie aus der Mitteilung hervorgeht. Bis 2036 rechnet das Unternehmen mit Aufwendungen von rund 5,9 Milliarden Franken. Die Investitionen sollen unter anderem Kapitalausgaben für den Bau von Rechenzentren, Betriebskosten im Zusammenhang mit den laufenden Versorgungs- und Anlagenkosten umfassen.

Den vollständigen Artikel finden Sie online
www.netzwoche.ch

Device Lifecycle Management: IoT-Geräte richtig verwalten – so geht's

Bei IoT-Lösungen spielt das Device Lifecycle Management eine wichtige Rolle. Wir verraten, welche acht Phasen ein IoT-Gerät durchlebt – und worauf dabei zu achten ist.

Das Internet of Things ist weiterhin auf dem Vormarsch und bietet Unternehmen viele Möglichkeiten zu neuen, innovativen Geschäftsmodellen. Während die Anzahl vernetzter Geräte rasant wächst, wird die einfache Verwaltung und Fernsteuerung von IoT-Hardware immer wichtiger. Aus diesem Grund kommt dem IoT Device Lifecycle Management eine grosse Bedeutung zu.

Ein ganzheitlicher Ansatz zur Verwaltung der eingesetzten Geräte hilft, deren Lebenszeit zu verlängern – und trägt so zum Erfolg des eigenen IoT-Use-Cases bei. Der Lebenszyklus eines IoT-Geräts unterscheidet sich je nach Branche und Anwendungsfall, dennoch kann er grob in diese Abschnitte unterteilt werden:

1. Bezug der Hardware (für Edge Devices oder Gateways)
2. Initiales Device Setup und Vulnerability Management
3. Device Provisioning
4. Connectivity Setup
5. Over-the-air-Updates
6. Monitoring
7. Wiederverkauf
8. Deprovisioning/Entsorgung

Im Folgenden soll auf diese einzelnen Phasen genauer eingegangen werden. Nicht zuletzt im Hinblick auf die Wahl einer geeigneten Cloud-Plattform ist es entscheidend, dass die nachstehend beschriebenen Prozesse weitestgehend automatisiert werden können. Nur so skaliert die eigene IoT-Lösung auch beim Einsatz vieler Devices.

1. Bezug der Hardware

IoT-Devices können über drei Arten mit dem Internet verbunden werden: direkt, über einen Field Gateway oder über ein Edge Device, das als Field Gateway dient. Ein Field Gateway kann etwa ein Mobilfunk-Gateway mit SIM-Karte sein oder auch ein Protokoll-Umwandler, der ein Nicht-IP-fähiges Gerät ans Internet anschliesst. Edge Devices besitzen in der Regel auch Gateway-Funktionalitäten, können darüber hinaus aber auch die Business-Logik lokal ausführen; etwa in Form von Containern, die von der Cloud geladen werden.

Für Field Gateways oder Edge Devices muss ein Hersteller evaluiert und eine Lieferkette etabliert werden. Je nach Cloud-Plattform gibt es ein Zertifizierungsprogramm, das die geeignete Hardware in einem Katalog ausweist.

2. Initiales Device Setup und Vulnerability Management

Anschliessend erfolgt ein initiales Device Setup – sprich, die Installation des Betriebssystems und allenfalls des Edge Frameworks auf den Edge Devices oder Field Gateways. Im Idealfall liefert der Hersteller bereits vorinstallierte Geräte inklusive allenfalls benötigter Lizenzen.

Eine besondere Herausforderung stellt schliesslich das Vulnerability Management des Software-Stacks dar: Es muss ein Prozess etabliert werden, in dem neu bekannt gewordene Sicherheitslücken schnell beurteilt und Patches zeitnah ausgespielt werden können. Unter Umständen bietet der Hardwarelieferant bereits entsprechende Möglichkeiten.

Auch das Device-Hardening – also das Erhöhen der Gerätesicherheit – sollte mit dem Hardwarelieferanten besprochen werden. Unter anderem muss sichergestellt sein, dass keine unnötigen Dienste auf dem Device laufen und alle Ports geschlossen sind. Dazu gehört auch die Absicherung des physischen Zugriffs auf die Geräte. Das Device Hardening wie auch entsprechende Test-Suiten sollten automatisiert werden.

3. Device Provisioning

Beim Device Provisioning wird das Gerät im IoT-System registriert und so konfiguriert, dass es Daten an das System sendet und sich im Unternehmensnetzwerk authentifiziert. Häufig geschieht das über Zertifikate, die auf dem Gerät installiert werden. Gewisse IoT-Plattformen bieten auch einen gesonderten Device-Provisionierungs-Service, mit dem dieser Schritt automatisiert werden kann.

Dennoch bleibt ein gewisser Implementierungsaufwand, um die Device-Provisionierung an die eigenen Prozesse und Systeme anzupassen. Entscheidend ist, ob das Gerät bereits vor der Auslieferung oder erst im Feld provisioniert wird: Bei einer Provisionierung im Vorfeld muss damit gerechnet werden, dass das Device über längere Zeit nicht mehr mit der Cloud verbunden ist – etwa, weil es in einem Lager aufbewahrt und erst später eingesetzt wird. Dies kann dazu führen, dass Zertifikate ablaufen, bevor das Device in Betrieb genommen wird.

Bei einer Provisionierung im Feld müssen Servicetechniker geschult werden, um das Device vor Ort provisionieren zu können. Wird für die Device-Authentifizierung ein Zertifikat verwendet, muss allenfalls eine eigene Public-Key-Infrastruktur aufgebaut werden.

Neben den Zugangsdaten wird bei der Provisionierung auch die initiale Konfiguration auf das Gerät gespielt. Auch hier sollte die Cloud-Plattform bereits einen Automatisierungsmechanismus anbieten, zum Beispiel mit Vorlagen (Device Templates), die automatisch auf gewisse Gerätegruppen angewendet werden.

4. Connectivity Setup

Grundsätzlich kann jedes IoT-Device (bzw. jeder Field Gateway) auf drei Arten mit dem Internet verbunden werden: über eine lokale Infrastruktur (LAN, WLAN), über einen eigenen Zugang durch Breitband-Mobilfunk oder über LPWAN (Low-Power Wide Area Network). In Zukunft wird auch der Zugang über Satelliten eine realistische Option sein.

Der Mobilfunk-Zugang kann idealerweise bereits vor der Auslieferung konfiguriert werden. Die grösste Herausforderung liegt in der Verwaltung der Mobilfunk-Verträge (inkl. Roaming) und der dazugehörigen SIM-Karten beziehungsweise eSIM-fähigen Devices. Beim Zugang via LAN/WLAN müssen für jedes einzelne Device die lokalen Netzwerk-Zugangsdaten konfiguriert werden inklusive möglicher Proxy- und DNS-Server. Dies

ist häufig nicht von vornherein möglich, da nicht bekannt ist, welches Gerät in welchem lokalen Netzwerk installiert wird. Gerade die Proxy-Server stellen dabei eine grosse Herausforderung dar, insbesondere wenn sie die TLS-Verbindung zum Cloud-Gateway unterbrechen (TLS Interception).

LPWAN-Verbindungen haben ihre ganz eigenen Herausforderungen und decken ihre eigene Kategorie von IoT-Use-Cases ab.

5. Over-the-air-Updates

Ist das Device im Feld installiert, konfiguriert und mit der Cloud verbunden, sollte es aus der Cloud aktualisiert werden können. Dies betrifft insbesondere Sicherheitspatches im Software-Stack, aber auch das Einspielen von neuen Server-TLS-Root-Zertifikaten des Cloud-Gateways oder Konfigurationsupdates. Bei Edge-Computing muss die Cloud-Plattform auch ein Lifecycle Management für Container-Images anbieten, die auf die Devices geladen werden sollten.

Im Fehlerfall sollte die Update-Funktionalität automatisch ein Rollback auf ein funktionierendes Setup machen können. Es sollte sichergestellt sein, dass mit der Remote-Update-Funktionalität auch Geräte mit alter Software noch aktualisiert werden können.

6. Monitoring

Solange IoT-Geräte aktiv sind, sollten sie über die Cloud überwacht werden. Man spricht hier von einem Flotten-Monitoring, da sowohl jedes einzelne Gerät als auch alle Gerätegruppen überwacht werden – sowohl im Hinblick auf den Gerätezustand als auch auf die Konfiguration, den Status von Edge-Containern und auf System-Parameter wie die Auslastung oder der Energieverbrauch.

Unter Umständen gehört auch ein automatisiertes Scanning auf Malware zum Monitoring der Edge Devices. Ebenso sollten Tests aus dem Device Hardening auch im Feld regelmässig durchgeführt werden können.

7. Wiederverkauf

Wie ein Auto in seinem Leben mehrfach den Besitzer wechselt, können auch IoT-fähige Geräte und Maschinen wiederverkauft werden. Dabei stellt sich die Frage, wie mit den eigenen Daten umgegangen werden soll: Welche Daten darf ein Käufer von einem IoT-Gerät einsehen, wenn er dieses erwirbt? Berücksichtigt meine IoT-Plattform, dass ein IoT-Gerät in seinem Leben den Besitzer beziehungsweise Mandanten wechselt?

8. Deprovisioning/Entsorgung

Bei der Deprovisionierung muss sichergestellt werden, dass das Gerät in der Cloud abgemeldet wird und somit die darauf gespeicherten Zugangsdaten ungültig sind. Dies stellt eine Herausforderung dar, falls die Cloud nur das Root-Zertifikat kennt und alle davon abgeleiteten Zertifikate akzeptiert werden.

ENTSCHEIDUNGSHILFE FÜR DIE RICHTIGE IOT-CLOUD-PLATTFORM

Das Booklet «Entscheidungshilfe für die richtige IoT-Cloud-Plattform» von bbv ist ein praktisches Nachschlagewerk für Verantwortliche von IoT-Projekten. Der Fokus des Booklets liegt vor allem auf Themen, die bei der Auswahl der Plattform oder generell zu Beginn eines IoT-Vorhabens eine wichtige Rolle spielen. Dazu bietet es zahlreiche Checklisten und Entscheidungshilfen an.
Die Inhalte des Booklets wurden aus mehreren IoT-Projekten gesammelt, dazu werden Best Practices aufgezeigt. Das Booklet behandelt unter anderem die Themen: Arten von IoT-Cloud-Plattformen, Funktionalität und Innovation, Konnektivität, Skalierbarkeit, Verfügbarkeit, Sicherheit, Vendor-Lock-in und Compliance.

Bestellen Sie das Booklet via Mail (info@bbv.ch) oder laden Sie es mit diesem QR-Code herunter.

bbv Software Services AG

Blumenrain 10
6002 Luzern
info@bbv.ch
+41 41 429 01 11

bbv
MAKING VISIONS WORK.

Mit privaten Cloud-Anbindungen das Risiko eines Cyberangriffs reduzieren

Auf dem Weg in die Cloud wird eine Vielzahl von Faktoren bis ins letzte Detail evaluiert. Die Connectivity zum Firmennetzwerk kommt dabei oft zu kurz. Jan Tschopp, Senior Product Manager Cloud Connectivity bei Swisscom, erklärt im Interview, wie eine sichere Verbindung in die Cloud das Risiko einer Cyberattacke reduziert. Interview: Tanja Mettauer

Jan Tschopp, Senior Product Manager Cloud Connectivity, Swisscom.

Vor Kurzem wurde bekannt, dass Swisscom Cloud-Anbindungen als AWS-Direct-Connect-Partner anbietet. Worum geht es dabei?
Jan Tschopp: Sobald Unternehmen anfangen, mit Private-Cloud-Anbietern wie Amazon Web Services (AWS) oder Microsoft Azure zu arbeiten, müssen diese Clouds ins bestehende Firmennetzwerk eingebunden werden. Entweder auf herkömmlichem Weg über das öffentliche Internet oder via private Anbindung. Bei einer Anbindung via Internet wird ein sogenanntes Site-to-Site-VPN erstellt. Bei einer privaten Anbindung werden die Daten über private Glasfaserkabel direkt in die Rechenzentren der Cloud-Anbieter geroutet. Das öffentliche Internet wird dabei umgangen. AWS bietet private Anbindungen unter dem Namen «Direct Connect» an, bei Azure nennt sich derselbe Service «Express Route», bei Google «Cloud Interconnect». Bei Swisscom nennt sich das entsprechende Produkt «Enterprise Connect – Cloud Access».

Sie sehen die Connectivity als einen kritischen Punkt?
Die meisten Firmen starten klein und gehen Schritt für Schritt in die Cloud, ohne gleich das gesamte Datacenter zu migrieren. Da der Workload damit über zwei oder mehrere Standorte verteilt läuft, ist es zentral, dass zwischen dem bestehenden Datacenter und der neuen Cloud eine zuverlässige Verbindung besteht.

Was ist der Vorteil einer privaten Anbindung?
Zum einen kann das Risiko einer Cyberattacke reduziert werden. Zudem sind private Cloud-Anbindungen typischerweise einfach- bis mehrfach-redundant aufgebaut. Firmen sind so besser vor einem Ausfall geschützt. Auch bieten private Anbindungen im Normalfall höhere Bandbreiten sowie stärkere Performance punkto Latenz und Jitter, sodass in der Cloud betriebene Applikationen möglichst störungsfrei laufen. Nicht zuletzt setzen regulierte Unternehmen, beispielsweise im Gesundheits- oder Finanzsektor, auf private Anbindungen, um ihre Patienten- oder Kundendaten stärker zu schützen.

Inwiefern kann das Risiko eines Cyberangriffs reduziert werden?
Anbindungen via Internet sind immer dem Risiko einer sogenannten Man-in-the-Middle-Attacke ausgesetzt. Dabei greift der Angreifer die Daten ab, ohne dass Sender oder Empfänger etwas davon merken. Durch eine private Anbindung kann dieses Risiko minimiert werden. Applikationen gelten generell als sicherer, wenn sie nicht über öffentliche IP-Adressen im Internet erreichbar sind.

Das klingt, als wären private Anbindungen teurer.
Tendenziell sind sie etwas teurer, ja. Je nach übertragener Datenmenge können Kosten aber wieder reduziert werden, da die Clouds Datenverkehr via Internet teurer verrechnen.

Kann man auch mehrere Clouds kombinieren?
Bei Swisscom können problemlos mehrere Clouds miteinander verbunden werden. Diese terminieren nicht am Kundenstandort, sondern bei uns im Backbone. Über das Onlineportal können diese Anbindungen beliebig untereinander verbunden werden. Man spricht hierbei auch von SDCI, Software-defined Cloud Interconnect.

Wieso sollen Unternehmen Swisscom als Cloud-Connectivity-Partner wählen?
Das Angebot von Swisscom ist einzigartig in der Schweiz. Swisscom kann als einzige AWS-Direct-Connect- und Azure-Express-Route-Partnerin das ganze Paket aus einer Hand anbieten. Vom Router vor Ort über die Swisscom-eigene Infrastruktur bis in die Rechenzentren der Cloud-Anbieter offerieren wir das gesamte Paket mit einem End-to-End-SLA. Zudem können unsere Kunden ihren Service binnen weniger Minuten im Onlineportal konfigurieren. Damit vereinfachen wir die Prozesse für unsere Kunden.

Das Interview finden Sie auch online
www.netzwoche.ch

Päckli sortieren mit DevOps

Am Glenfis-Cloud-Talk in Zürich haben ein Experte, ein Anwender, ein Provider und ein Agile-Coach über das Thema DevOps referiert. Eine wichtige Erkenntnis des Anlasses: Eine DevOps-Transformation ist vor allem ein Change-Projekt. Autor: Marc Landis

Glenfis-Cloud-Talk im Restaurant «Clouds» in Zürich.

DevOps ist heute in aller Munde. Manche Unternehmen sehen es als Tool, als Software oder als Job-Profil, etwa demjenigen des DevOps-Engineers. Da aber DevOps vor allem eine neue Unternehmenskultur mit sich bringt, greift diese Betrachtung zu kurz, wie Schulungsanbieter Glenfis im Programm seines Cloud-Talks vom 26. Oktober unter dem Motto «DevOps Xperience» verlautbarte.

Das Ziel der Referenten des Cloud-Talks im Zürcher Restaurant «Clouds» war es denn auch unter anderem, Antworten auf die Frage zu finden, ob DevOps eine Modeerscheinung sei oder das neue Paradigma der IT. Ausserdem sollte beantwortet werden, wo Schweizer IT-Organisationen in ihrer DevOps-Transformation stehen, wie sie dabei vorgehen, welche Stolperfallen und Erfolge sie erleben und welchen Nutzen sie generiert.

DevOps beschreibt bekanntlich den Ansatz, der die Prozesse zwischen Softwareentwicklung und operationalen IT-Teams automatisiert und optimiert, damit Software schneller und zuverlässiger erstellt, getestet und freigegeben werden kann. Ausserdem geht es bei DevOps darum, die Barrieren zwischen traditionell isolierten Entwicklungs-Teams und den operationellen IT-Teams einzureissen.

Das aber erfordert einen Kulturwandel, der wie andere Change-Prozesse einen Change-Manager erfordert. DevOps-Experte Martin Thalmann von Monum nannte ihn in seinem Referat «Change Agent». Ausserdem erklärte Thalmann die drei Wege, die gemäss Lehrbuch die Transformation der IT hin zu DevOps weisen, beschrieb vier Dimensionen, die davon betroffen sind, und schloss sein Referat mit fünf Umsetzungsempfehlungen ab.

Den vollständigen Artikel finden Sie online
www.netzwoche.ch

Drei Wege, vier Dimensionen, fünf Mantras

Die drei Wege in den «DevOps-Himmel» beschrieb Thalmann mit Flow, Feedback und Continual Learning. Im Flow machen Projektleiter von DevOps-Transformationsprojekten den Workflow etwa via Kanban-Boards sichtbar. Bei Feedbacks geht es darum, den Entwicklungsprozess so weit zu beschleunigen, dass Rückmeldungen innerhalb von 60 Minuten zur Verfügung stehen. Der dritte Weg führt in Scrum über das kontinuierliche Lernen via Retrospektiven. Diese sind grundlegende Elemente des Scrum-Frameworks.

Die vier betroffenen Dimensionen sind Technik, Prozesse, Kultur und Organisation. «DevOps sind dann erfolgreich, wenn man alle vier Dimensionen im Griff hat», sagte Thalmann.

Zur Umsetzung notierte Thalmann fünf Merksätze, man könnte sie auch Mantras nennen:

1. Behandle Transformation als agiles Projekt!
2. Qualifizierte Change Agents sind elementar!
3. One Size does not fit all!
4. Behalte den Fokus auf technische Exzellenz!
5. Veränderung braucht Zeit!

Es folgte ein Referat von Kyle Krüsi, der den Weg Microsofts hin zu DevOps beschrieb. Ihren Anfang nahm diese Reise 2014, als Satya Nadella als CEO übernahm.

Besondere Aufmerksamkeit am Glenfis-Cloud-Talk genoss aber Marc Sallin von der Post. Er berichtete von einem DevOps-Projekt, in dem er in seinem Team in der Post-IT die Software für die Päckli-Sortierung nach DevOps-Grundsätzen komplett neu entwickelte oder in Sallins Worten: «Die Software musste herausfinden, welcher Bote welches Päckli zustellen muss.»

Sallin nannte aber auch Herausforderungen, die mit einem DevOps-Projekt einhergehen – etwa, dass oft Führungskräfte fehlten, um DevOps-Projekte auf zusätzliche Bereiche im Unternehmen auszudehnen. Ausserdem sprach er über den Dunning-Kruger-Effekt, der beschreibt, wie (Führungs-)Mitarbeitende bei einem (DevOps-)Projekt «dreinreden», ohne über die nötige Kompetenz zu verfügen.

Ein weiteres Problem könne die Maturität der bereits vorhandenen Plattform sein. Niemand mag gerne Veränderungen, insbesondere dann nicht, wenn das bestehende System ja noch immer funktioniert.

Eine weitere Herausforderung sei, dass es innerhalb von Organisationen oft an Vertrauen gegenüber IT-Projekten mangle, etwa aufgrund der diffusen Angst, ein neues effizienteres System könnte einen den Arbeitsplatz kosten.

Public-Cloud-Projekt des Bundes: keine vorsorglichen Massnahmen

Das Bundesverwaltungsgericht muss klären, ob es eine gesetzliche Grundlage für das Public-Cloud-Projekt des Bundes gibt. In einer Zwischenverfügung hat das Gericht nun entschieden, keine vorsorglichen Massnahmen gegen die Bundesverwaltung zu verhängen. Autor: René Jaun

Den vollständigen Artikel finden Sie online
www.netzwoche.ch

Das Bundesverwaltungsgericht verhängt keine vorsorglichen Massnahmen gegen das Public-Cloud-Projekt der Bundesverwaltung. In der Medienmitteilung zu seiner Zwischenverfügung schreibt das Bundesverwaltungsgericht, dass keine Notwendigkeit für den Erlass solcher Massnahmen bestehe. Eine Privatperson hatte das Gericht dazu aufgefordert, das Projekt zu stoppen, falls die entsprechende gesetzliche Grundlage fehle, wie das Onlinemagazin «Republik» berichtete.

Die Verwaltungsrechtspflege sehe weder eine generell-abstrakte Normenkontrolle noch eine Popularbeschwerde vor, führt das Bundesverwaltungsgericht aus. Der Beschwerdeführer könne daher nur ein schutzwürdiges Interesse bezüglich der Bearbeitung von eigenen Personendaten geltend machen. Eine unmittelbare Gefahr, dass die Bundeskanzlei Daten auslagere, die den Kläger beträfen, könne verneint werden, schreibt das Gericht weiter.

Bundeskanzlei: Leistungsbezug kann starten

Die Bundesverwaltung wiederum gab Ende September 2022 bekannt, dass die Verträge mit den fünf Hyperscalern (Alibaba, Amazon Web Services, IBM, Microsoft und Oracle) unterschrieben seien. Aufgrund des Zwischenentscheids des Bundesverwaltungsgerichts entschied die Bundeskanzlei nun, dass die Verwaltungseinheiten entsprechende Dienste über diese Verträge beziehen dürfen. In der Mitteilung betont die Bundeskanzlei, dass vor dem Leistungsbezug umfangreiche Abklärungen durchgeführt würden. Zudem seien Bezüge im Rahmen der ausgehandelten Verträge optional.

Sowohl das Gericht als auch die Bundeskanzlei merken an, dass der Zwischenentscheid vor Bundesgericht angefochten werden könne. Zudem läuft das Hauptverfahren weiter, in dessen Rahmen das Gericht klären muss, ob es eine ausreichende gesetzliche Grundlage für das Public-Cloud-Projekt des Bundes gibt. Dieses Verfahren werde wohl noch einige Zeit dauern, schreibt die Bundeskanzlei.

Patzer bei der Ausschreibung

Ein Blick in interne Dokumente des Bundes offenbarte bereits Anfang 2022, dass die Behörden auf dem Weg zum Public-Cloud-Projekt mehrere fragwürdige Entscheide gefällt hatten. Der Bund habe «interne Warnungen zum heiklen Beschaffungsprozess ignoriert, Fehler in der Ausschreibung begangen – und dazu die kommunikativen und medialen Risiken der Public-Cloud-Ausschreibung komplett unterschätzt», berichtete «Republik».

Fragen zum Datenschutz etwa waren im Vorfeld der Ausschreibung durchaus ein Thema. Mehrere Behörden, darunter das Justiz- und Polizeidepartement (EJPD) und der Datenschutzbeauftragte (EDÖB), meldeten dem Bericht zufolge entsprechende Bedenken an. Auszüge aus internen Mails zeigen, dass der US-amerikanische Cloud Act und der chinesische MLPS-2.0-Standard zur Sprache kamen. Das EJPD habe derweil gefordert, nur unproblematische Daten für die Lagerung in der Public Cloud zuzulassen. In der Ausschreibung seien diese heiklen Themen dann aber nicht weiter definiert worden.

Das Bundesverwaltungsgericht in St. Gallen.
Bild: peterruggle.ch

Switch lanciert Cloud speziell für Hochschulen

Switch lanciert mit der «Switch Cloud» einen neuen Cloud-Dienst, der auf spezifische Bedürfnisse des Schweizer Bildungssektors zugeschnitten ist. Für das Angebot arbeitet die Stiftung mit Phoenix Systems zusammen. Autor: Yannick Züllig

Visho Jesudasan, Head of Sourcing, Architecture & Operations, Switch.

Den Artikel finden Sie auch online
www.netzwoche.ch

Die Stiftung Switch kündigt eine Cloud-Lösung namens «Switch Cloud» an. Diese soll auf die speziellen Bedürfnisse des Bildungs-, Forschungs- und Innovationssystems zugeschnitten sein, wie die Stiftung mitteilt.

Hintergrund des Projekts sei, dass aktuelle Cloud-Angebote die Bedürfnisse von Forschungseinrichtungen und des Bildungswesens «nur teilweise» abdeckten. Da Switch seit bald 40 Jahren als Digitalisierungspartnerin mit entsprechenden Institutionen zusammenarbeite, kenne man diese Bedürfnisse genau.

Angebot zur gemeinsamen Weiterentwicklung

Wer die Switch Cloud nutzt, bekommt auch die Möglichkeit, sich in den Weiterentwicklungsprozess einzubringen. «Nutzende unserer Cloud-Lösung haben Zugang zu einem einzigartigen Zusammenarbeitsmodell, indem sie gegenwärtige und künftige Herausforderungen in die Ausgestaltung und Weiterentwicklung von Switch Cloud einbringen können», sagt Visho Jesudasan, Head of Sourcing, Architecture and Operations von Switch.

Gehostet in der Schweiz

Die Switch Cloud setze hohe Massstäbe an Rechtssicherheit, Datenhoheit und Datenschutz. Sie stehe unter der vollen Kontrolle der Stiftung im Interesse ihrer Destinatäre, teilt Switch mit.

Die Cloud-Lösung werde nach dem neuesten Stand der Technik in ISO-zertifizierten Rechenzentren von Green in Schlieren und Lupfig betrieben und weiterentwickelt. Sie laufe auf Hardware-Technologie von IBM. Der redundante Betrieb an zwei Schweizer Standorten sei sowohl hochperformant als auch hochverfügbar und flexibel skalierbar.

Partnerschaft mit Green, IBM und Phoenix

Für die Realisierung und den Betrieb der Cloud arbeite man in einer strategischen Partnerschaft mit dem Zürcher Hosting-Anbieter Phoenix Systems zusammen. Sowohl Green wie IBM sind langjährige Technologiepartner von Phoenix. Phoenix Systems verantwortet die Bereitstellung der Infrastruktur und Switch ist für die darauf aufbauenden Cloud-Services und den Gesamtbetrieb zuständig. Die Stiftung ist zudem persönliche Ansprechpartnerin der Kundinnen und Kunden und hilft ihnen bei der Integration.

Geplant ist, dass in der zweiten Hälfte 2023 erste Projekte auf der Switch Cloud realisiert werden.

Switch ist nicht gewinnorientiert. Die Stiftung fungiert als Netzwerk-, Security- und Cloud-Provider für die Schweizer Hochschulen und betreibt die Registry für die Schweizer Domainnamen (.ch und .li). Switch beschäftigt rund 140 Mitarbeitende an ihrem Geschäftsstandort in Zürich.

Private-Cloud-Betrieb für SAP-Systeme in der Schweiz – Erfolgsgeschichte Siegfried AG

In vielen Anwendungsbereichen gewinnen stark standardisierte Public-Cloud-Lösungen immer mehr an Bedeutung. Anders als bei vielen SAP-Kunden. Sie müssen ihre Systeme aufgrund interner Massgaben oder regulatorischer Vorgaben in einem Umfeld betreiben, das den gewünschten Grad an Individualisierung sicher, stabil und wirtschaftlich ermöglicht.

Siegfried AG, Zofingen

Die im aargauischen Zofingen beheimatete Siegfried AG (SWX: SFZN) hat sich in den vergangenen Jahren durch eine konsequent umgesetzte Strategie zu einem weltweit führenden Pharmazulieferer entwickelt. Als Contract Development & Manufacturing Organisation (CDMO) bietet Siegfried anderen Unternehmen der Pharmaindustrie spezialisierte Dienstleistungen – von der Entwicklung einzelner Wirkstoffe bis zur Produktion fertig formulierter Medikamente in unterschiedlichsten Darreichungsformen. Rund 3600 Expertinnen und Experten an derzeit elf Standorten in Europa, Nordamerika und Asien bilden die Erfolgsfähigkeit, mit der Siegfried die strategische Entwicklung voranträgt.

Die Betätigungsfelder von Siegfried gestalten sich seit jeher sehr dynamisch. Betrachten wir dazu speziell die vergangenen 30 Monate, so haben wirtschaftliche und geopolitische Realitäten die Organisation mit ganz speziellen Herausforderungen konfrontiert. Nach Ausbruch der Coronapandemie hatte Siegfried nämlich nicht nur spontane Auswirkungen wie regionale Lockdowns, Versorgungsengpässe sowie Turbulenzen an den Währungsmärkten zu bewältigen. Das Unternehmen wurde gleichzeitig zu einem wesentlichen Erfolgsfaktor bei der Bekämpfung der Pandemie. Während die Hersteller auf behördliche Freigaben hinwirkten, baute Siegfried blitzschnell die Abfüllung einzelner Covid-Impfstoffe auf und ermöglichte dadurch eine rasche, weltweite Verfügbarkeit der Impfdosen in enormen Mengen. Parallel beschleunigte Siegfried die strategische Expansion und kündigte im Spätherbst 2020 an, in der Region Barcelona zwei spezialisierte Produktionsstandorte von Novartis zu übernehmen.

Heute, rund 22 Monate nach Abschluss dieser Transaktion, zeichnet sich inmitten der geopolitischen Turbulenzen folgendes Bild: Siegfried hat mit der Implementierung einer topmodernen Installation von SAP S/4HANA den digitalen Kern für die effiziente Integration von Prozessen, Informationen, Personen und Expertensystemen geschaffen und realisiert Schritt für Schritt weitere Rollout-Projekte sowie strategische Initiativen in der Industriedigitalisierung. Innflow ist Implementierungspartner für diese neue Lösung. Die erfolgreiche Umsetzung dieses sehr anspruchsvollen Programms in einem dynamischen und weltweit hochgradig regulierten Umfeld bedingt ein ebenso sicheres und zuverlässiges wie flexibles und leistungsfähiges Betriebsmodell für die SAP-Lösungen von Siegfried.

Innflow Private Cloud:
Agile Leistung made in Switzerland

Die Beweggründe dafür, SAP-zentrische Informationssysteme einem Private-Cloud-Anbieter anzuvertrauen, können vielseitig sein. Die strategische Geschäftsentwicklung von Siegfried muss bezüglich des Systembetriebs einen besonders hohen Grad an Zuverlässigkeit, Flexibilität und Skalierbarkeit sowie direkte Kommunikationswege und kurze Reaktionszeiten einfordern. Aus operativer Sicht ausschlaggebend ist, dass regulatorische Vorschriften nach Current Good Manufacturing Practice (cGMP) zwingend einzuhalten sind und deren Einhaltung jederzeit nachgewiesen werden kann. Weiter hat der Schutz vor Cyberkriminalität eine absolut zentrale Bedeutung. Und letztlich muss der Systembetrieb in einem wirtschaftlich attraktiven, wettbewerbsfähigen Rahmen nach den aktuellen Regeln der Technik erfolgen.

Um diesen Anforderungen Rechnung zu tragen, ist die Innflow Private Cloud aus operativer und organisatorischer Sicht in einer mehrstufigen Qualitätssicherungsstruktur aufgebaut:

1. SAP Certified in SAP HANA Operations
2. SAP Certified in Hosting Operations
3. SAP Certified in Cloud and Infrastructure Operations
4. Jährliche Prüfung und kundenspezifische Zertifizierung nach ISAE 3402 Typ II
5. Kundenspezifische Prüfungen und Zertifizierung für cGMP
6. Zertifizierung der Support-Organisation nach ISO 9001

Die mit diesen Zertifizierungen einhergehenden technischen und organisatorischen Strukturen stehen als Garant für Sicherheit, Leistungsfähigkeit, Zuverlässigkeit und Wirtschaftlichkeit für den Private-Cloud-Systembetrieb rund um die Uhr. Ergänzend dazu sind jedoch auch Agilität und Pragmatik gefordert, wo immer diese Qualitäten angewendet werden dürfen. Innflow steht als lokaler Partner mit internationaler Ausrichtung sofort bereit, wenn kurzfristig Erweiterungen in der Systemlandschaft oder

Die Siegfried AG in Zofingen.

neue Verbindungen zu diversen Cloud-Lösungen erforderlich sind. Diese Verbindung aus professionellen Private-Cloud-Services und einer persönlichen Betreuung für kundenspezifische Anforderungen bilden die optimale Grundlage für den hybriden Systembetrieb: SAP S/4HANA sowie selektive Zusatzlösungen in der Private Cloud, verbunden mit ergänzenden Lösungen aus dem Public-Cloud-Angebot von SAP und weiteren Herstellern.

Künstliche Intelligenz und Automatisierung

Wirtschaftlichkeit und Zuverlässigkeit im Private-Cloud-Systembetrieb werden bei Innflow unter anderem durch den gezielten Einsatz von Cloud-Management-Systemen erreicht, die Pflegearbeiten mithilfe künstlicher Intelligenz weitgehend automatisiert umsetzen und darüber lückenlose Rechenschaft ablegen. Dieses Vorgehen schafft eine einzigartige Betriebssicherheit und -stabilität, ermöglicht dabei aber gleichzeitig, flexibel auf individuelle Kundenanforderungen einzugehen. Etwa dann, wenn eine grössere Systemaktualisierung nicht fix nach Cloud-Release-Planung durchgeführt werden kann, weil dadurch kundenseitig ein Konflikt mit anderen Projekten innerhalb eines Programms entstehen würde, oder nicht zuletzt, weil dem Kunden auf einen gewissen Zeitpunkt hin schlicht die Ressourcen fehlen, um erforderliche Tests, Dokumentationen, gegebenenfalls Validierungen und Schulungen sowie mögliche Anpassungen an Umfeldsystemen vorzunehmen. Auch Siegfried profitiert regelmässig von der Flexibilität, die das hybride Betriebsmodell für die SAP-Systemlandschaft mit sich bringt.

Die heute schon ausgefeilten Automatisierungsmechanismen werden durch das Engineering-Team von Innflow fortlaufend erweitert. Zusätzlich zu Effizienzgewinnen lassen sich dadurch weitere Sicherheitsstufen abbilden, konsequent anwenden und den Kunden gegenüber transparent belegen.

Wirtschaftlichkeit beginnt im Kleinen

Weltweit planen unzählige SAP-Kunden den Schritt hin zu einer Public-Cloud-Lösung mit SAP und werden dadurch in ungeahnter Weise von einer konsequenten Standardisierung ihrer Organisation und Geschäftsprozesse profitieren. Für Unternehmen sowie für Organisationen der öffentlichen Hand, die aus strategischen und/oder regulatorischen Überlegungen andere Wege verfolgen möchten, bilden Angebote wie die Innflow Private Cloud langfristig eine hervorragende Alternative als Betriebsmodell.

Längst nicht alle Firmen unterstehen strikten, internationalen Regulatorien wie etwa dem cGMP-Regelwerk. Folglich lässt sich die Innflow Private Cloud auch mit einfachen strukturierten Service Level Agreements effizient nutzen. Angefangen bei temporären Systemen als Sandbox oder für die Realisierung eines Proof of Concept über Systeme im Projektbetrieb bis zu grösseren SAP-zentrischen Lösungen, die nicht 24/7, sondern lediglich zu den effektiven Einsatzzeiten in Mitteleuropa garantiert verfügbar sein müssen, können pro Lösungselement unterschiedlich umfangreiche Leistungen und Verfügbarkeitsgarantien festgelegt, angewendet und auch unterjährig jederzeit flexibel angepasst werden. Wo dieser Komfort erwünscht ist und angewendet werden darf, entstehen zeitgemässe Lösungsarchitekturen, auf deren Basis sich hervorragend arbeiten lässt.

Die Schweiz gilt weltweit als sicherer Aufbewahrungsort für die digitale Vertrauenssphäre von Unternehmen und Behörden. Mit der gebotenen Achtsamkeit werden Energie- und Kommunikationsversorgung auch in den aktuell etwas turbulenteren Zeiten sichergestellt sein.

Innflow AG

Blegistrasse 1 | CH-6343 Rotkreuz
www.innflow.com

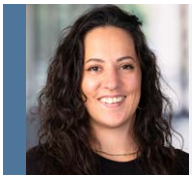
Die in Rotkreuz ZG ansässige Innflow AG zählt zu den führenden Anbietern SAP-zentrischer Informationssysteme in der Schweiz. Innflow verbindet Dienstleistungen für Organisations- und Prozessberatung nahtlos mit SAP-Projekt-, Support- und Betriebsleistungen. SAP-Lösungen von Innflow werden weltweit eingesetzt und unterstützen zahlreiche Unternehmen und Organisationen der öffentlichen Hand dabei, ihre Geschäftsziele optimal zu erreichen.

Warum die richtige Backup-Strategie für das revDSG so wichtig ist

Mit dem Ausrollen des neuen Datenschutzgesetzes sollen Kundendaten besser geschützt werden. Unternehmen sind jetzt gefordert und müssen verschiedene Massnahmen umsetzen.

Am 1. September 2023 tritt das total-revidierte Datenschutzgesetz (revDSG) in Kraft. Es ersetzt die bisherige Fassung von 1993. Die Änderungen beinhalten insbesondere Anpassungen an die technologischen Entwicklungen der vergangenen Jahre mit einem Fokus auf besseren Schutz von persönlichen Daten.

Betroffen von diesen Änderungen ist jedes Unternehmen, das personenbezogene Daten verarbeitet. Ausser den technischen und juristischen sind auch einige organisatorische Schutzmassnahmen erforderlich, wie etwa ein Backup-Konzept. Mit der richtigen Backup-Strategie sind Unternehmen nicht nur konform im Rahmen des revDSG, sondern auch effektiv bei der Sicherung von Firmendaten.



Die Autorin
Debora Urso, Content Marketing Manager, Alltron

Daten sind die wertvollsten Ressourcen für ein Unternehmen

Unternehmen sollten darauf Wert legen, ihre wichtigste Ressource, nämlich ihre Daten, zu schützen. Gefahren für die Daten von Unternehmen gibt es auf diversen Ebenen:

- Ökologische Gefahren wie Feuer und Wasser
- Cyberangriffe wie etwa Ransomware-Attacken
- Nicht korrekt abgespeicherte Dokumente

Um solchen Gefahren entgegenzuwirken, wird Unternehmen empfohlen, regelmässig Backups ihrer Systeme zu erstellen. Dadurch werden nicht nur die Daten zusätzlich gesichert, sondern auch die Zeit minimiert, in der ein Betrieb wegen der genannten Faktoren ausser Gefecht gesetzt werden kann.

Mit der passenden Backup-Strategie zum Rundumschutz

Wichtig ist nicht nur, dass die Daten des Unternehmens gesichert werden, sondern auch wie und wo. Bei einem Ausfall des Systems kann das Wie und Wo entscheidend sein. Oftmals wird von der 3-2-1-Strategie gesprochen.

Mindestens drei Sicherungen der Daten: Unternehmen sollten beim Sichern der Daten immer vom Worst-Case-Szenario ausgehen. Je mehr Datenkopien vorhanden sind, desto unwahrscheinlicher ist es, dass die Sicherungen unabhängig voneinander ausfallen.

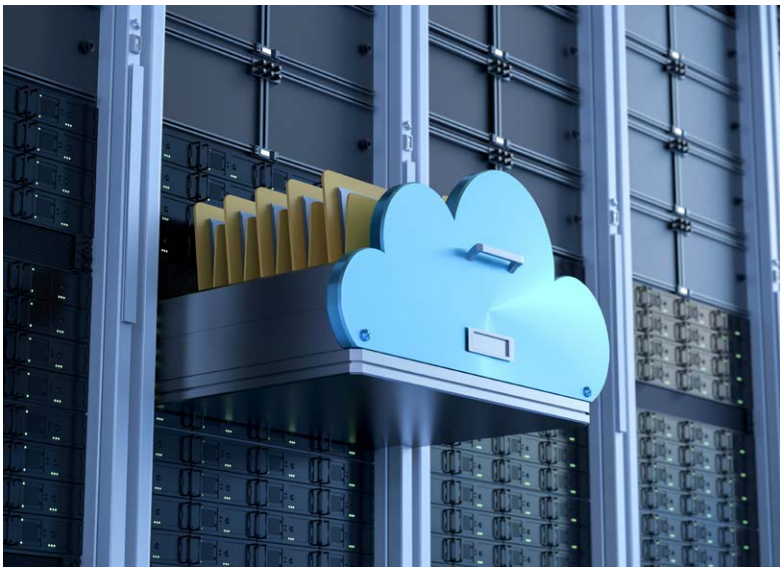
Die Sicherungen auf mindestes zwei verschiedenen Datenträgern: Alle Backup-Technologien und Datenträger bringen ihre eigenen Fehleranfälligkeiten mit sich. Damit die Eventualität eines Ausfalles minimiert wird, sollten die Backups auf verschiedenen Datenträgern erstellt werden. Es besteht die Option, lokale Speicher, wie etwa ein NAS, zu nutzen oder auf die Cloud auszuweichen. Wichtig ist, dass alle Backup-Anbieter dementsprechende Sicherheitsmechanismen anbieten.

Eine Sicherheitskopie an einem externen Standort: Wenn Backups nicht physisch voneinander getrennt sind, gehen sie im Katastrophenfall alle verloren. Dieses Risiko kann eliminiert werden, wenn mindestens eine Sicherung extern abgelegt ist, sei es in der Cloud oder in einem externen Datencenter.

Eine Sicherung sollte offline gespeichert werden: Damit eine Unabhängigkeit vom Internet erstellt werden kann, sollte mindestens eine Sicherung offline verfügbar sein. Dies kann in Form von externen Festplatten geschehen.

Fazit

Die Massnahmen des revDSG sind sehr zeitintensiv, somit empfiehlt sich, diese frühzeitig in Angriff zu nehmen. Mit einer durchdachten und auf die Firma angepassten Backup-Strategie ist ein wichtiger Teil der Anforderungen des revDSG gedeckt und Unternehmen können so Datenverluste verhindern und Ausfallzeiten minimieren.



«Ein grosser Vorteil der Nutzung von Cloud-Diensten ist die Flexibilität»

Die Sicherung von Unternehmensdaten ist ein komplexer, vielschichtiger Prozess. Eine gute Backup-Strategie umfasst daher verschiedene Lösungsaspekte, wie Oliver Widmer, Specialized Sales IT Security bei Alltron, im Interview sagt. Interview: Yannick Züllig

Was ist die für Unternehmen wichtigste Änderung im neuen Datenschutzgesetz?
Oliver Widmer: Es gibt eine ganze Reihe von relevanten Veränderungen. Eine besonders wichtige Veränderung ist hervorzuheben: das obligatorische Verzeichnis der Bearbeitungstätigkeiten. Dies bedeutet, dass Unternehmen künftig vom Gesetzgeber nicht nur verpflichtet sind, sich an den Datenschutz zu halten, sondern auch nachweislich dokumentieren müssen, wie sie dies gewährleisten.

Wie regelmässig müssen Backups erstellt werden, um Unternehmen effektiv zu schützen?
Unternehmen müssen sich grundsätzlich Gedanken machen, was ein akzeptabler Zeitraum zwischen den Backups ist – wie viel Datenverlust also akzeptabel ist. Diese RPO (Recovery Point Objective) genannte Messgrösse kann für jedes Unternehmen oder auch unterschiedliche Systeme sehr individuell sein. In letzter Zeit hat sich hier auf der technischen Schiene einiges getan. Einige Backup-Lösungen bieten die Möglichkeit an, die Nutzdaten ohne Unterbrechung zu sichern, die restlichen Systemdaten (etwa das Betriebssystem) hingegen nur beispielsweise ein Mal pro Tag. Mit Acronis Cyber Protect kann etwa eine Applikation oder ein Pfad bestimmt werden, dessen Daten bei jeder Änderung sofort gesichert werden. Damit kann das RPO praktisch komplett auf null reduziert werden.

Sind Naturkatastrophen oder Cyberangriffe aktuell ein grösseres Risiko für Unternehmensdaten?
Beides sind legitime Gefahrenquellen, die unterschiedliche Lösungsansätze erfordern. Da Naturkatastrophen in der Regel seltener vorkommen und lokal gebunden sind, kann dieses Risiko bereits mit einer Datensicherung an unterschiedlichen Standorten (geo-replication) stark gemindert werden. Cyberangriffe hingegen können jederzeit und ortsunabhängig erfolgen, ausserdem sind diese oftmals zielgerichtet und werden mit starker krimineller Energie durchgeführt. Die Bedrohungslage ist sehr komplex und erfordert mehrschichtige Schutzkonzepte, um Unternehmen gegen die unterschiedlichen Arten von Cyberangriffen zu schützen.

Ist es sinnvoller, zunächst in mehr Hardware- oder cloudbasierte Backups zu investieren? Und warum?
Zu einer guten Backup-Strategie sollte immer beides gehören.

Oliver Widmer, Specialized Sales IT Security, Alltron.

Lokale Backups helfen dabei, nach einem Desaster rasch Daten wiederherstellen zu können – ohne den Flaschenhals Internetleitung. Zusätzlich dazu sollte immer auch eine Kopie der Daten an einem anderen Standort vorhanden sein, etwa in der Cloud, um auch unabhängig des Standorts auf die Backups zugreifen zu können. Ein grosser Vorteil der Nutzung von Cloud-Diensten ist die Flexibilität. Cloud-Dienste erfordern keine grosse Investition und es können flexibel zusätzliche Ressourcen und Services dazugebucht werden.

Wie weit kann die 3-2-1-Strategie ausgebaut werden, bevor zu viele Redundanzen entstehen?
Natürlich können weitere Kopien, Medientypen (etwa Tape) und Standorte hinzugefügt werden, was aber die besagten Redundanzen schafft. Hier kommt es sehr darauf an, welche Anforderungen an die Verfügbarkeit der Daten nach einem Desaster bestehen. Mit mehr Redundanzen können je nach Art des Desasters schneller die Daten wiederhergestellt werden – das lässt sich in der Messgrösse RTO (Recovery Time Objective) festlegen.

Das Dossier finden Sie auch online
www.netzwoche.ch

«Man muss bewusst entscheiden, wo man die Cloud einsetzt und welche Daten man darin speichert»

Die Smart Factory der Fachhochschule OST soll den Wertschöpfungsprozess einer digitalisierten Produktion abbilden. Roman Hänggi spricht über die Hintergründe und erklärt, wo die Schweiz auf dem Weg zur Industrie 4.0 steht und welche Rolle die Cloud dabei spielt. Interview: Yannick Züllig

Im Oktober hat die OST die Smart Factory in Buchs eröffnet. Was genau macht so eine Smart Factory?
Roman Hänggi: Unsere Smart Factory besteht aus drei Standorten: Rapperswil, St. Gallen und Buchs. Die smarte Fabrik an diesen drei Standorten ist ein Abbild der Produktion der Zukunft. Sowohl physisch als auch digital. Die Maschinen in der Fabrik produzieren physisch das sogenannte «OST-Gadget», ein Handy-Ladegerät. Dabei sammeln wir sämtliche Daten, die während des Produktionszyklus und der Qualitätsprüfung entstehen, speichern sie digital ab und verwenden sie zur weiteren Analyse. Dieser digitale Zwilling hilft uns, weitere Optimierungen zu realisieren.

Wie profitieren die Studierenden der OST davon?
Unsere Studierenden lernen alle diese Elemente so zu verbinden, dass man möglichst effizient und zukunftsgerichtet produzieren kann. Das geschieht in verschiedenen Modulen und Vorlesungen, wo die Studierenden erleben, wie die Fabrik funktioniert und wie man die Produktion der Zukunft effektiv gestalten kann. Auch wird die Smart Factory von den Studierenden, im Rahmen von Semester- oder Bachelorarbeiten, stetig weiterentwickelt.

Wie unterscheiden sich die drei Standorte?
Die jeweiligen Fertigungsschritte werden an unterschiedlichen Standorten vollzogen. In Rapperswil wird das Gehäuse des «OST-Gadgets» gespritzt, inklusive eineindeutiger Identifikation und Serialisierung. In Buchs verbauen wir anschliessend die Elektronik im Gehäuse, und der Standort St. Gallen ist verantwortlich für den digitalen Prozess dieser Fertigung.

ZUR PERSON

Roman Hänggi ist seit 2016 an der Fachhochschule OST als Professor für Produktionsmanagement tätig. Nach dem Studium an der ETH und dem Doktorat an der HSG arbeitete er 25 Jahre lang in der Industrie (Leica, Hilti, Bosch, Arbonia) und hat internationale Führungserfahrung. Die Transformation der Industrie durch Lean, Digitalisierung und industrielle Services sind die Schwerpunkte seiner Tätigkeiten in der Praxis und Forschung. Publikationen und Fachbücher im Bereich «Lean» und «Smarte Fabrik» fassen die Erfahrungen und Ergebnisse zusammen.

Wie sind diese Standorte miteinander vernetzt?
Wir nutzen hierzu ein zentrales ERP und eine zentrale Cloud, wo wir die verschiedenen Daten ablegen. Verschiedene datentechnische Anbindungen und Schnittstellen zwischen Maschine, Cloud und ERP sind im Einsatz.

Welche Rolle spielt dabei die Cloud?
Die Cloud ist ein Element, das wir für das digitale Abbild der Produktionskette nutzen. Aber dieser digitale Zwilling besteht nicht nur aus der Cloud, dazu gehören auch viele Businessprozesse mit umfassenden Daten rundherum.

Welche Rolle spielt die Cloud in der digitalen Transformation der Industrie im Allgemeinen?
Die Cloud spielt eine sehr zentrale Rolle. Für mich ist die Cloud ein technisches Hilfsmittel für die Kollaboration und Datenspeicherung. Mit Kollaboration meine ich hier ein Produktionsnetzwerk, wie es die Smart Factory mit den Standorten in Buchs, St. Gallen und Rapperswil abbildet. Im Vergleich zur traditionellen Produktion an einem einzelnen Standort müssen die verschiedenen Punkte eines Produktionsnetzwerks miteinander verknüpft sein und gemeinsam effizient arbeiten. Mit einer Cloud als technisches Hilfsmittel für den Austausch von Daten ist die Zusammenarbeit innerhalb des Netzwerks überhaupt realisierbar.

Wie müsste diese Zusammenarbeit aussehen, wenn es gar keine Cloud gäbe?
Es gibt natürlich auch andere Wege, um Daten auszutauschen. In gewissen Fällen würde es den Produktionsprozess komplizierter machen, wenn ständig Daten hin und her geschickt werden müssten. Ganz viele Datenströme müssten individuell aufgesetzt werden. Mit der Cloud geht das alles einfacher und es kommt zu weniger Datenredundanzen.

Im Zusammenhang mit der Cloud werden immer wieder Bedenken geäussert, wenn es um den Datenschutz geht. Gibt es solch Bedenken auch in der Fertigungsindustrie?
Das ist sicherlich auch ein Thema. Wichtig ist, dass man sich bewusst entscheidet, wo man die Cloud einsetzt und welche Daten man darin speichert. Das bedingt eine Abwägung von Risiken.

Die Cloud ist sicherheitstechnisch weder gut noch schlecht – es kommt darauf an, wie man sie nutzt. Es braucht eine klare Strategie, bei der festgelegt ist, wohin man mit welchen Daten geht. Dazu gehört auch ein Sicherheitskonzept. Gewisse Daten sollte man unter Umständen aus Sicherheits- oder Vertraulichkeitsgründen besser nur lokal speichern.

Was gehört sonst noch in ein industrielles Cloud-Konzept?
Gerade in einer Fabrik entstehen immer sehr viele Daten, weil alle Maschinen ständig all ihre Aktivitäten dokumentieren. Nicht alle diese Daten gehören in die Cloud. Ausserdem sollte man sich auch Gedanken zur Geschwindigkeit der Umsetzung und zu den Kosten seiner Strategie machen.

Gibt es ein ungefähres Verhältnis, wie viel in der Cloud und wie viel On-Prem passieren sollte?
Das kann man nicht direkt sagen. Das genaue Verhältnis hängt sehr stark vom jeweiligen Use Case und der Art des Produktionsnetzwerks ab.

Welche Trends beobachten Sie derzeit im Bereich der industriellen Cloud?
Ein grosser Trend ist die Vereinfachung von Integrationsprozessen. Unterschiedliche Maschinen von unterschiedlichen Herstellern produzieren Daten in vielen verschiedenen Formaten und nach verschiedenen Standards. All diese Daten kommen an einem Ort zusammen, nämlich in der Cloud. Und vielerorts wird daran gearbeitet, diese Integrationsleistung einfacher und effizienter zu gestalten. Ein zweiter grosser Trend ist sicherlich Data Analytics. Denn die Cloud an sich ist ja eigentlich nur ein Datenspeicher. Aber wenn die Daten einmal in der Cloud sind, dann muss man ja noch immer etwas damit machen. Da gibt es verschiedene Softwarelösungen, sei es Business Intelligence, seien es Machine-Learning-Ansätze oder sei es eine direkte Anbindung an ein ERP-System – die Daten müssen zu relevanten Informationen transferiert werden.

Sehen Sie da eher die Industrie in Zugzwang oder sollten Cloud-Anbieter mehr industriespezifische Lösungen anbieten?
Das ist eine sehr relevante Frage. Wenn ich mir die heutigen grossen Cloud-Anbieter anschaue, dann sehe ich eine Tendenz dazu, dass versucht wird, die Industrie aus einer IT-Sicht besser zu verstehen. Da hat sich sicherlich etwas getan in letzter Zeit. Man versucht, die industriellen Themen mehr und besser anzugehen. Gleichzeitig wachsen in der Industrie selbst das Verständnis und die Bereitschaft zur Nutzung der Cloud, zumal sich Kosten sparen lassen, wenn man seine Produktionsprozesse analysiert und mithilfe der Cloud digitalisiert. Das zeigt sich auch daran, dass immer mehr über Standards diskutiert wird. Denn verbindliche, herstellerübergreifende Standards machen die zuvor erwähnten Integrationsprozesse deutlich einfacher.

Hat die klassische Fabrik heute noch eine Chance oder braucht es zwingend eine Digitalisierung der Produktion?
Die Fabrik der Zukunft ist sicher digital, aber nicht nur digital. Das Fundament sind schlanke, verschwendungsarme Prozesse, die

«Die Cloud ist sicherheitstechnisch weder gut noch schlecht – es kommt darauf an, wie man sie nutzt.»

Roman Hänggi, Professor für Produktionsmanagement, Ostschweizer Fachhochschule

«on top» noch digitalisiert werden. Lean Management gewinnt heute eine noch grössere strategische Bedeutung. Die Digitalisierung hat natürlich auch einen Einfluss darauf, wie man diese fundamentalen Prozesse gestaltet. Eine wirklich effiziente Produktion optimiert sich dauernd, und der beste Weg dazu ist, aus Daten zu lernen. Die Digitalisierung hilft dabei, viel mehr Daten zu generieren und aus diesen auch mehr Informationen zu ziehen, die dann die Optimierung ermöglichen. Es besteht also eine Wechselwirkung zwischen den Prozessen und den Daten.

Wie stehen die Chancen der Schweiz, sich in dieser modernen Produktionswelt zu behaupten?
Es ist meine tiefe Überzeugung, dass der Produktionsstandort Schweiz in der Zukunft extreme Chancen hat.

Warum?
Wenn Sie eine Fabrik der Zukunft, also eine effiziente Fabrik bauen wollen, dann brauchen Sie stabile Prozesse und Sie müssen die Digitalisierung und digitale Tools im Griff haben. Es braucht Automation, etwa durch Robotik, und man muss die Produktionstechnologien vollständig verstehen. Man muss also Arbeitskräfte aus vielen Fachdisziplinen zusammenbringen, etwa den Maschinenbauer, Softwareentwicklerinnen, Elektroingenieure, Produktionsmitarbeiterinnen oder Betriebswirtschaftler. Alle Disziplinen müssen miteinander arbeiten, um eine solche Fabrik der Zukunft zu realisieren. Und da hat die Schweiz eine enorme Stärke, mit ihrem Ausbildungssystem und ihren teamorientierten Ansätzen. Hierarchien sind schlecht für die Fabrik der Zukunft, denn Daten und Systeme kennen keine Hierarchiegrenzen. Es braucht einen flexiblen Bottom-up-Ansatz, natürlich mit klaren Zielen und Visionen, aber danach braucht es einen Team-basierten Ansatz, der die unterschiedlichen Kompetenzen zusammenbringt, um die Fabrik der Zukunft zu bauen. Generell braucht es jedoch über all diese Felder hinweg gesehen noch mehr Digitalkompetenz.

Wie kann man diese Digitalkompetenzen stärken?
Im Kanton St. Gallen gibt es etwa die IT-Bildungsoffensive. Diese verfolgt genau diesen Ansatz, dass über alle Ausbildungsniveaus hinweg mehr Digitalkompetenz geschaffen wird. Dabei werden bestehende Strukturen, etwa eine Berufslehre oder ein Fachhochschul-Studiengang, um digitale Kompetenzen erweitert, anstatt einen Studiengang «Digitalisierung» zu schaffen. Ich glaube, schweizweit ist das eine einzigartige Initiative, um das Ziel der erhöhten Digitalkompetenz zu erreichen.

Wo steht die Schweiz aktuell im Bereich der digitalisierten Industrie?
Die Schweiz ist hier führend oder gehört sicher zu den führenden Playern in diesem Bereich. Dabei spielt der Industrieverband Swissmem mit der Initiative 2025 eine entscheidende Rolle. Auch haben wir sehr viele innovative Firmen hier in der Schweiz und vor allem in der Ostschweiz, gerade aus dem Mittelstand, die sehr viel Neues ausprobieren und umsetzen. Unsere Universitäten und Fachhochschulen haben den Zug auch nicht verschlafen und sind dabei, diese Zukunft der digitalen Industrie mitzugestalten und nach vorne zu bringen. Wir in der Schweiz haben sicher unseren Beitrag zur Fabrik der Zukunft geleistet. Das reicht jedoch noch lange nicht aus, wir müssen uns dauernd weiterentwickeln. Wer stehen bleibt und sich nicht permanent hinterfragt, verliert.

Das Interview finden Sie auch online
www.netzwoche.ch

Roman Hänggi, Professor für Produktionsmanagement, Ostschweizer Fachhochschule.

Mit der Industrie 4.0 soll alles schneller, schlanker, digitaler und effizienter werden. Gibt es dabei auch Dinge, die man kritisch betrachten sollte?
Ich glaube, es braucht einen gesunden Realismus. Wir müssen eine saubere Erwartungshaltung an den Tag legen, denn es passiert viel, aber nicht alles passiert über Nacht. Man kann nicht einfach eine Software kaufen und dann wird alles besser in der Firma. Unternehmen müssen einen Weg finden, die Tools der Digitalisierung so einzusetzen, dass es auch in ihren Betrieb passt. Und am Ende bleibt der Mensch entscheidend. Technologie ist ein Mittel zum Zweck und nicht das Ziel. Digitalisierung ist so kompliziert, weil jede Firma ihren eigenen Weg finden muss, um an ihr eigentliches Ziel zu kommen. Nicht alles geht so schnell, wie man es sich immer wünscht. Es ist eine Transformation, die sehr genau gemanagt werden muss. Die digitale Transformation muss integraler Teil der Geschäftsführung sein, sie muss zielorientiert und anwendungsfallorientiert sein.

Und ist die Schweiz hier auf einem guten Weg?
Auf einem sehr guten Weg, würde ich sagen. Wir müssen einfach weitermachen und den eingeschlagenen Weg weitergehen. Denn die digitale Transformation ist nie abgeschlossen. Aber wenn wir unseren bisherigen Weg weitergehen, dann sehe ich viele Chancen für die Industrie in der Schweiz.

ORIA von ITpoint: Schweizer Cloud- und Managed IT Services

ORIA ist die Marke für das Cloud- und Managed-Services-Angebot von ITpoint und ermöglicht Unternehmen, IT ganzheitlich als zuverlässige, sichere und agile Dienstleistung zu beziehen. Wir begleiten Sie bei der Transition von Ihrer heutigen IT-Infrastruktur in die Cloud.

Hohe Skalierbarkeit mit der Schweizer ORIA Enterprise Cloud

ITpoint betreibt und hostet Ihre Windows-, Linux-, IBM-i-/AIX-Betriebssysteme, -Anwendungen und -Datenbanken (SQL und Oracle) auf der hochskalierbaren ORIA Enterprise Cloud in Schweizer Rechenzentren. Sie profitieren von höchster Leistung, marktführender Verfügbarkeit und Sicherheit, klaren Prozessen und Service Level Agreements. Darüber hinaus profitieren Sie von unserem Kundenportal mit transparenter und detaillierter Abrechnung über Ihre effektiv genutzten Cloud-Ressourcen und vielfältigen Reporting-Möglichkeiten zu Ihrer Cloud-Infrastruktur.

Wir bieten:

- **Infrastructure-as-a-Service** inklusive Betriebssysteme Windows, Linux, IBM i und IBM AIX
- **Cloud-Backup-Lösungen** wie Ransomware Protected Backup, Tape Backup, OnPrem to Cloud Backup und Microsoft 365 Backup
- **Disaster-Recovery-Lösungen** für Cloud- und OnPrem-Infrastruktur
- Firewall, Web Application Firewall, Secure Application Delivery und Load Balancing
- **Sicherheitslösungen** wie Ransomware Protection, Schwachstellenmanagement, Endpoint Detection & Response (EDR), Network Detection & Response (NDR), Syslog Management, Auditing, Managed SIEM und SOC (Security Operation Center)
- **Datenbankmanagement** mit Microsoft SQL und Oracle
- Active Directory, File Services, Exchange, Citrix- und RDS Published Desktop sowie Application Hosting und Management
- **Digital Workplace** als umfassende Lösungen für Ihre Arbeitsplätze und Mobilgeräte mit Microsoft 365 Endpoint Management/Intune, Samsung Knox und BlackBerry
- **Microsoft-365-Online-Services** für Exchange, Teams etc. sowie Teams Enterprise Voice (Ersatz Ihrer Telefonieanlage vor Ort)
- **Microsoft Azure** für Hybrid-Cloud-Szenarien

Sie kümmern sich um Ihr Kerngeschäft – wir uns um Ihre IT

Mehrere Faktoren entscheiden, ob der eigene Betrieb Ihrer IT-Infrastruktur für Ihr Unternehmen sinnvoll ist. So oder so: Mit der Übergabe der Betriebsverantwortung an uns können Sie an Sicherheit, Flexibilität und Wirtschaftlichkeit gewinnen. ITpoint ist ISO-20000- und 27001-zertifiziert, nach ISAE 3402 Type 2 auditiert und entspricht den FINMA-Outsourcing-Bestimmungen für Banken und Versicherungen sowie den GxP-, GAMP5- und Computer-System-Validation-Bestimmungen und Empfehlungen für die Pharmaindustrie.

Empowering people to do what they love

Die IT nimmt in der Business-Welt immer mehr Raum ein. Dabei wird heute schnell vergessen, dass wir alle Menschen sind – einzigartige Menschen. Wir hören unseren Kundinnen und Kunden zu und entwickeln gemeinsam Lösungen, die sie weiterbringen, indem wir die IT in jeder Hinsicht verbessern, indem wir ändern, wie Dinge gemacht werden, und indem wir positive Erlebnisse auch über die IT hinaus bieten.

Unsere Kunden können sich auf ihre Leidenschaft, ihr Kerngeschäft fokussieren, weil wir sie mit unserer Leidenschaft, der IT, auf dem Weg zum Erfolg unterstützen. Was auch immer die Leidenschaft unserer Kundinnen und Kunden ist: Mit motivierten, qualifizierten Mitarbeitenden und smarten IT-Lösungen erzeugen wir Freude und unterstützen sie auf ihrem Weg zum Erfolg.

itpoint | ORIA PRIME MANAGED SERVICES

Trusted IT for Business

ITpoint Systems AG

Riedstrasse 1 | 6343 Rotkreuz | +41 41 798 80 80
info@itpoint.ch | itpoint.ch

NorthC-Group drängt in den Schweizer RZ-Markt

Den vollständigen Artikel finden Sie online
www.netzwoche.ch

aob. Die niederländische NorthC-Group hat die Datacenter- und Connectivity-Sparte von Netrics übernommen – und ist somit neu auch in der Schweiz präsent. Die Unternehmensgruppe kaufte von Netrics drei Rechenzentren, zwei in Münchenstein und eines in Biel. Über diese Datenstandorte bietet NorthC Schweiz nun Cloud-Lösungen sowie Colocation- und Konnektivitätsdienste an, wie das Unternehmen mitteilt. Als Konnektivitätspartner setze das Unternehmen hierzulande unter anderem auf Swisscom, Sunrise und Quickline.

Die nach Tier-3-Standards gebauten Rechenzentren garantieren laut Mitteilung höchste Sicherheit und sind über ein Fiber-Backbone untereinander verbunden. Zusätzlich ermögliche die Anbindung an wichtige Internet-Exchange-Punkte Hochgeschwindigkeits-Datenverbindungen. Die angebotene Hybrid Cloud setze sich aus einer Public Cloud, einer Private Cloud sowie Infrastrukturen in externen Rechenzentren zusammen. Für die Public Cloud arbeite man mit Google Cloud, AWS, Microsoft Azure, IBM Cloud, Oracle Cloud und Open Telekom Cloud zusammen.

Equinix erweitert Rechenzentrum in Zürich

Den vollständigen Artikel finden Sie online
www.netzwoche.ch

jor. Equinix hat sein Datacenter ZH4 in der Stadt Zürich ausgebaut. Der US-amerikanische Rechenzentrumsbetreiber ergänzte den Standort um eine weitere Halle mit einer Colocation-Fläche von 850 Quadratmetern und über 200 Cabinets, wie das Unternehmen mitteilt. Es handle sich um den fünften Ausbau des Rechenzentrums. In der Schweiz betreibt Equinix fünf Rechenzentren, davon drei in Zürich und zwei in Genf.

Das Datacenter ZH4 beherbergt unter anderem die Matching Engine der Schweizer Börse Six Swiss Exchange. Das Rechenzentrum bietet laut Mitteilung einen direkten Zugriff auf ein globales Ökosystem aus über 10 000 Unternehmen sowie aus Netzwerken, Clouds und Services.

Das neu ausgebaute Datacenter sei denn auch im Einklang mit der Nachhaltigkeitsstrategie des Betreibers konzipiert. Bis 2030 strebe man einen klimaneutralen Betrieb an, heisst es. Dies entspricht einer Vorgabe der EU-Kommission, wonach alle in der Europäischen Union betriebenen Datacenter bis 2030 CO2-neutral operieren sollen.

Hosttech lässt RZ ISO 27001 zertifizieren

Den vollständigen Artikel finden Sie online
www.netzwoche.ch

mla. Hosttech hat sein Rechenzentrum Datarock für den Betrieb von Datacenter- und Cloud-Services ISO/IEC 27001 zertifizieren lassen. So ist für die Kunden sichergestellt, dass die Datenschutzrichtlinien eingehalten und die Systemsicherheit gewährleistet ist, wie das Unternehmen mitteilt.

«Das Datacenter Datarock wurde bereits vor der Zertifizierung nach den ISO-27001-Standards geführt», sagt Marcel Meuwly, Qualitätsmanager von Hosttech. Jedoch habe die Erarbeitung des Informationssicherheits-Managementsystems einen beträchtlichen Arbeitsaufwand gefordert. Dies vor allem, da alle internen Prozesse ISO-gerecht dokumentiert werden mussten. «Das Resultat zeigt aber, dass es sich gelohnt hat und wir nun ein strukturiertes und effizientes Managementsystem nutzen können», bestätigt Hosttech-CTO Manuel Kälin.

Datarock befindet sich in Nottwil in einem ehemaligen Militärspital 15 Meter unter der Erdoberfläche. So seien die physische Sicherheit, die Energieversorgung und die Abschirmung von Umwelteinflüssen gewährleistet.

Energieeffizienz von Rechenzentren stagniert

Den vollständigen Artikel finden Sie online
www.netzwoche.ch

ych/rja. Seit 2014 machen Rechenzentren bezüglich ihrer Energieeffizienz keine nennenswerten Fortschritte mehr, wie aus einer Studie des Uptime Institute hervorgeht. Demnach verzeichneten Rechenzentrumsbetreiber in den Jahren 2007 bis 2014 die grössten Fortschritte, indem der durchschnittliche PUE-Wert von 2,5 auf 1,65 sank. Seitdem stagniert der Wert weitgehend – 2021 betrug er 1,57.

PUE steht für «Power Usage Effectiveness». Man berechnet den Indikator, indem man den Gesamtenergieverbrauch des Rechenzentrums durch die Energie teilt, die nur für den Betrieb der IT-Systeme (Server, Speicher, Netzwerk) benötigt wird.

Um diesen Indikator weiter zu senken, sind laut der Studie erhebliche Änderungen erforderlich: Bei bestehenden Einrichtungen käme eine Aufrüstung mit einem hocheffizienten Kühlsystem infrage; bei künftigen Rechenzentren könnten hingegen neue Ansätze respektive neue Technologien zu mehr Energieeffizienz beitragen, beispielsweise eine Kühlung durch direkten Kontakt mit Flüssigkeiten oder Feststoffen.

Das Gebäude, in dem sich das Heizkraftwerk und das Rechenzentrum der EPFL befinden, ist mit Photovoltaik-Modulen bedeckt.
Bild: Alain Herzog/EPFL

Die EPFL heizt jetzt mit der Abwärme ihres Rechenzentrums

Die EPFL hat ihr neues Heizkraftwerk eingeweiht. Betrieben wird es nicht mehr mit Heizöl, sondern unter anderem mit Wasser aus dem Genfersee. Dieses kühlt ein Rechenzentrum, dessen Abwärme trägt dann wiederum zur Beheizung des Campus bei. Autor: Yannick Chavanne, Übersetzung: René Jaun

Nach dreijähriger Bauzeit hat die ETH Lausanne (EPFL) ein neues Heizkraftwerk eingeweiht. Das Besondere daran: Es nutzt unter anderem die im Rechenzentrum entstehende Abwärme, um den Campus zu beheizen. Laut der EPFL ist die Anlage ein wichtiger Schritt auf dem Weg zur CO2-Neutralität.

An der Einweihungsfeier am 8. September erklärte Matthias Gäumann, Vizepräsident Operations, die Funktionsweise der komplexen Infrastruktur. Demnach ermöglicht ein kombiniertes System aus Pumpen im Genfersee, Wärmetauschern, Sonnenkollektoren sowie einer Nutzung der vom Datenzentrum abgegebenen Wärme, den Campus zu kühlen und zu beheizen. Im Gegensatz zu früheren Anlagen werde im neuen System überhaupt kein Heizöl mehr verwendet.

Den CO2-Fussabdruck reduzieren

Die neue Anlage, die in Zusammenarbeit mit Bouygues errichtet wurde, liefert 54 Prozent des gesamten Energiebedarfs der EPFL. Dazu kommen weitere 40 Prozent aus Strom und 6 Prozent Gas. Die neue Anlage komme genau zum richtigen Zeitpunkt, betonte EPFL-Präsident Martin Vetterli in seiner Rede. Sie ermögliche eine «absolut substanzielle» Reduzierung des CO2-Fussabdrucks der Hochschule. Gisou van der Goot, Vizepräsidentin für nachhaltige Transformation an der EPFL, führte aus, dass ein mit Gas oder Öl betriebenes Kraftwerk einen viermal höheren CO2-Fussabdruck hätte.

Ihre Energie bezieht die Anlage auch von Photovoltaikmodulen auf dem Dach und an allen Fassaden des Wärmepumpen-Heizkraftwerks. Zudem pumpt das System Wasser mit einer konstanten Temperatur von 7 Grad aus dem Genfersee (aus einer Tiefe von 75 Metern). Das Wasser fliesst durch eine 1 Kilometer lange Leitung mit einem Durchmesser von 1,1 Metern zu vier riesigen neuartigen Wärmepumpen, die das Wasser durch den thermodynamischen Prozess der Kompression, Kondensation, Entspannung und Verdampfung auf 67 Grad erhitzen können.

Den vollständigen Artikel finden Sie online
www.netzwoche.ch

RZ kühlen und Abwärme weiterverwenden

Das Rechenzentrum hat eine Fläche von fast 1000 Quadratmetern, die Platz für zwölf Servergassen bietet. Auf Anfrage erklärt Philippe Morel, Leiter der IT-Infrastruktur und des IT-Betriebs, dass durch die Türen der Racks mit Seewasser gekühltes, gefiltertes Industriewasser zirkuliert. Das Wasser, das mit einer Temperatur zwischen 24 und 28 Grad aus den Racks kommt, wird dann zu den Wärmepumpen umgeleitet, um zur Beheizung des Campus beizutragen.

Die Speicher- und Rechenkapazität des Zentrums werde schrittweise auf 4 Megawatt steigen. Der PUE-Wert (Energieeffizienzindikator) dieses Rechenzentrums, das über dem Heizkraftwerk angesiedelt ist, beträgt zunächst 1,15 und soll künftig auf 1,1 sinken. Zur Erinnerung: Je niedriger der PUE-Wert, desto effizienter ist das Rechenzentrum. Laut dem Uptime Institute stagniert die Energieeffizienz von Rechenzentren seit mehreren Jahren.

Das neue System werde künftig auch wissenschaftlich genutzt, teilt die EPFL mit. So wollen das Ecocloud-Zentrum und das Energiezentrum der EPFL gemeinsam ein Projekt starten, um die CO2-Emissionen aus dem Betrieb des Rechenzentrums zu minimieren. Dieses soll die Photovoltaikpanels der Heizzentrale und die auf dem Campus befindliche Speicherbatterie nutzen und direkt vom Rechenzentrum aus gesteuert werden.

«In der aktuellen Situation ist es beruhigend zu wissen, dass wir ein heizölfreier Campus sind, beinahe ohne Gas auskommen und dank der neuen Heizzentrale grösstenteils erneuerbar unterwegs sind», sagt Gisou van der Goot und ergänzt: «Das ist ein wichtiger Meilenstein auf dem weiteren Weg.»

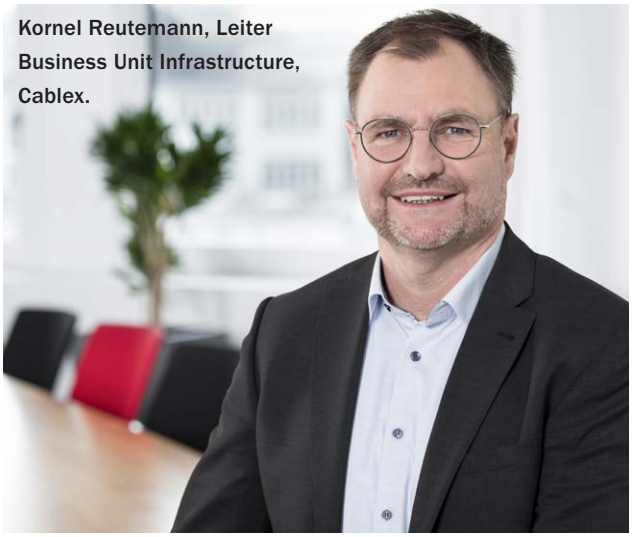
Was Cablex im Geschäft mit Rechenzentren vorhat

Die Swisscom-Tochter Cablex ist seit zwei Jahren im Geschäft mit Field Services. Darunter fallen Installationen und Wartungen von ICT-Netzwerken in Rechenzentren. Wie sich das Unternehmen in diesem Markt positionieren will, erklärt Kornel Reutemann. Interview: Joël Orizet

Cablex entstand vor 21 Jahren durch die Auslagerung der Bauabteilung von Swisscom. Sie sind aber auch ausserhalb des Netzbaus tätig: Laut Ihrer Website bieten Sie etwa ICT-Gesamtlösungen an, ebenso wie Swisscom und zahlreiche ICT-Dienstleister. Wie wollen Sie sich im Wettbewerb abgrenzen?
Kornel Reutemann: Unser Dienstleistungsangebot fokussiert sich auf die Realisierung und den Betrieb von ICT-Netzen und -Systemlösungen. Nebst den IMACD-Diensten (Install, Move, Add, Change und Dispose) umfasst das Portfolio auch Projekt- und Rolloutsowie Incident-Management und Unterhalt. Wir sind ein kompetenter, schweizweit agierender Partner für ICT-On-Site-Projekte. Durch ein engmaschiges Servicenetz mit lokalen Mitarbeitenden und Logistik Drop Points können wir anspruchsvollste Dienstleistungsvereinbarungen erfüllen.

Vor zwei Jahren hat Cablex das Servicegeschäft von Swisscom übernommen – inklusive rund 1000 Servicetechnik-Mitarbeitende. Swisscom begründete die Auslagerung der Sparte mit der rückläufigen Nachfrage nach Einsätzen vor Ort. Wie hat sich das Auftragsvolumen seither entwickelt?
Positiv. Unser Kundenstamm und Projektvolumen sind in den vergangenen Monaten stetig gewachsen. Einen grossen Mehrwert bieten dabei die schweizweite Präsenz von Cablex, Sicherheitszertifizierungen und unsere technische Erfahrung. Wir dürfen feststellen, dass die Qualität und Zuverlässigkeit bei unseren Kunden geschätzt werden.

Seit der Übernahme dieses Geschäfts bietet Cablex Field Services im B2B-Markt an. Dazu gehören Installationen, Wartungen und Störungsbehebungen von ICT-Netzwerken vor Ort sowie auch in Rechenzentren. Was planen Sie in diesem Geschäftsfeld?
Die Schweiz hat ein gutes Marktumfeld für Datacenter-Anbieter und es wurden in den letzten Jahren viele neue Rechenzentren gebaut. Dieser Trend wird sich fortsetzen. Insbesondere dort, wo Kunden ihre Hardware in die Datacenter verlagern (Colocation), setzt der ICT-Service von Cablex auf. In Kombination mit unserer Elektroinstallationsabteilung können wir den Kunden ein komplettes Lifecycle-Portfolio für die Basisinfrastruktur eines Rechenzentrums anbieten, inklusive Lösungen für eine smarte Energieversorgung. Diesen Bereich bauen wir weiter aus.


Kornel Reutemann, Leiter Business Unit Infrastructure, Cablex.

Fernwartungen gehören längst zum Standardrepertoire von ICT-Dienstleistern. Support vor Ort könnte sich langfristig zu einer Nischendienstleistung entwickeln. Was sagen Sie dazu?
Auch in Zeiten der Digitalisierung ist der persönliche Service und Support von Mensch zu Mensch ein wichtiger Bestandteil der Kundenerlebniskette. Wir sind überzeugt, dass es die Hände vor Ort auch in Zukunft braucht. Die heutigen Technologien wie AR eröffnen neue Möglichkeiten bei den On-Site-Einsätzen. Die Digitalisierung generiert zudem viele physische Geräte wie Sensoren, die vor Ort installiert, verbunden und entstört werden müssen.

Angenommen, die kabellose Datenübertragung aus dem Weltall macht Breitbandanschlüsse über Glasfaser obsolet: Was passiert mit Cablex?
Das satellitenbasierte Breitbandnetz ist ein interessanter Ansatz, insbesondere für schwer zugängliche Gegenden. Ich sehe es als Ergänzung zum heutigen Infrastruktur-Setup, gehe aber nicht davon aus, dass es die heutige physische Infrastruktur in den nächsten Jahren obsolet macht. Zu gross sind heute noch die Hindernisse für ein flächendeckendes Netz bezüglich Kapazität, Strahlung, Kosten und Verfügbarkeit.

Das vollständige Interview finden Sie online
www.netzwoche.ch

Finanzdienstleister stehen bei Multi-Cloud am Anfang

Die Finanzbranche hinkt bei der Multi-Cloud-Einführung hinterher. Dies, obwohl die Befragten in einer Nutanix-Studie Multi-Cloud als das ideale IT-Betriebsmodell ansehen. Autor: Marc Landis

Den vollständigen Artikel finden Sie online
www.netzwoche.ch

Der US-amerikanische Anbieter von Multi-Cloud-Lösungen Nutanix hat die Ergebnisse seines vierten weltweiten Enterprise Cloud Index (ECI) für die Finanzindustrie vorgelegt. Die Studie misst den Fortschritt von Unternehmen und Einrichtungen bei der Cloud-Einführung, wie das Unternehmen in einer Mitteilung schreibt. Die Umfrageergebnisse zeigen, dass in der Finanzindustrie weniger Unternehmen Multi-Cloud-Umgebungen einführten als in jeder anderen untersuchten Branche. Der Anteil der Implementierungen soll sich jedoch in den nächsten drei Jahren von 26 Prozent auf 56 Prozent mehr als verdoppeln.

Keine Cloud bei 59 Prozent

Von den ECI-Teilnehmern aus der Finanzindustrie betreiben 31 Prozent weiterhin nicht-cloudfähige Tier-3-Rechenzentren als einzige IT-Infrastruktur. 59 Prozent nutzen laut Studie überhaupt keine Public-Cloud-Dienste, was «vermutlich den grossen in der Vergangenheit getätigten Investitionen in die Anwendungslandschaft und der hochregulierten Natur der Branche geschuldet» sei.

Die Komplexität des Managements über Cloud-Grenzen hinweg bleibe eine der grössten Challenges für Finanzdienstleister: 84 Prozent der Befragten stimmen darin überein, dass ein einfacheres und übergreifendes Management von Multi-Cloud-Infrastrukturen Erfolgsvoraussetzung ist, während 50 Prozent Sicherheitsbedenken als Hindernis für das Multi-Cloud-Modell anführen.

Wie es weiter heisst, führen 82 Prozent an, dass ein hybrides Multi-Cloud-Modell – also ein IT-Betriebsmodell mit mehreren privaten wie auch öffentlichen und untereinander interoperablen Cloud-Umgebungen – ideal sei, um die wichtigsten Herausforderungen im Zusammenhang mit Sicherheit, Interoperabilität und Datenintegration zu adressieren. «Da Datensicherheit und operationale Resilienz für Finanzdienstleister im Zentrum der Aufmerksamkeit bleiben, müssen sie sich mit Lösungen für die hybride Multi-Cloud beschäftigen, die mit integriertem Management und eingebauter Sicherheit sowie der Fähigkeit ausgestattet sind, Apps schnell und kosteneffizient über Cloud-Infrastrukturen hinweg zu verschieben», sagt dazu Anand Akela, VP of Product and Solutions Marketing von Nutanix, hinsichtlich der von seinem Unternehmen angebotenen Lösungen nicht ganz uneigennützig in der Mittteilung.

Herausforderungen der Finanzindustrie in der Cloud

Die Finanzbranche kämpfe beim Thema Multi-Cloud mit Herausforderungen, heisst es weiter; dazu zählten Sicherheit (50 Prozent), Datenintegration über Cloud-Grenzen hinweg (46 Prozent) und Leistungseinbussen mit Netzwerk-Overlays (43 Prozent). Beinahe 78 Prozent geben demnach einen teilweisen Mangel an erforderlichen IT-Kompetenzen an, um den aktuellen Unternehmensanforderungen gerecht zu werden.

Die IT-Führungskräfte seien sich jedoch bewusst, dass es keinen One-size-fits-all-Ansatz für die Cloud gebe, was die hybride Multi-Cloud laut der grossen Mehrheit der Studienteilnehmer (82 Prozent) zum idealen Modell macht.

Sicherheit als erste Priorität

Die wichtigsten IT-Prioritäten der Finanzindustrie liegen laut Mitteilung in den nächsten 12 bis 18 Monaten in der Erhöhung des Sicherheitsniveaus (54 Prozent), der Verbesserung des Multi-Cloud-Managements (49 Prozent) sowie der Entwicklung und Implementierung cloud-nativer Technologien (47 Prozent). Auf die Frage, was ihre Unternehmen aufgrund der Pandemie anders gemacht hätten als früher, antworteten die Teilnehmer wie folgt:

- 70 Prozent erhöhten demnach ihre Ausgaben, um ihr Sicherheitsniveau zu steigern.
- 64 Prozent gaben mehr Geld für Selfservices auf Basis künstlicher Intelligenz aus, um einen höheren Automatisierungsgrad zu erreichen.
- 64 Prozent investierten in die Modernisierung ihrer Infrastruktur.

«Die Pandemie hat die Abhängigkeit von transnationalen Cloud-Lösungen weiter erhöht»

Digitale Souveränität ermöglicht es Unternehmen und Privaten, wieder selbst über ihre Daten zu bestimmen. Der Weg dorthin ist aber nicht einfach, solange die Abhängigkeit der Clouds von Bigtech nicht reduziert wird. Martin Andenmatten von Eurocloud Swiss erklärt, was es dafür braucht.

Interview: Marc Landis

Was ist digitale Souveränität?

Martin Andenmatten: Unter digitaler Souveränität versteht man heute allgemein selbstbestimmtes Handeln im digitalen Raum. Das Wort «Souveränität» kommt aus dem Französischen und bedeutet «Unabhängigkeit». In seinen Ursprüngen werden dabei die Unabhängigkeit und Selbstbestimmung von Staaten verstanden. Der souveräne Staat hat die Macht, seine Gesetze und seine Regierungsform selbst zu bestimmen. Im digitalen Universum ist dieser Begriff jedoch nicht so leicht abzugrenzen und zu definieren. Durch die Unabhängigkeit des Cyberspace haben Regierungen in diesem Ökosystem kaum noch Autorität. Dadurch konnte sich die digitale Globalisierung praktisch ungehindert entwickeln. Grenzen und Gesetze wurden ignoriert und haben es einflussreichen Internetakteuren ermöglicht, ihre eigenen Regeln aufzustellen und sogar als «vollständig digitalisierte Nationen» eingestuft zu werden. Die im Jahr 2013 publik gewordene Snowden-Affäre über massenhafte Abhöraktionen der NSA machten die Risiken deutlich, die mit der fehlenden Kontrolle des digitalen Raums verbunden sind. Im Jahr 2015 warf der Skandal zwischen Facebook und Cambridge Analytica ein Schlaglicht auf die betrügerische Nutzung personenbezogener Nutzerdaten durch multinationale Unternehmen. Diese grossen Unternehmen haben sich in Bezug auf Vertraulichkeit eher gleichgültig gezeigt. Die Bewegung für digitale Souveränität zielt nun darauf ab, einen Teil der im digitalen Raum ausgeübten Macht zurückzugewinnen. Insbesondere auf europäischer Ebene ist die digitale Unabhängigkeit inzwischen zu einem festen Begriff geworden. Man will damit unabhängige Lösungen entwickeln– insbesondere auch in der Cloud, die im Kern den Umgang mit sensiblen Daten sichern.

Warum ist digitale Souveränität wichtig?

Die Frage nach der Sicherheit in der Cloud greift heute viel zu kurz. Was Unternehmen wirklich wollen, ist die direkte Kontrolle ihrer Daten. Die Pandemie hat die Abhängigkeit der Unternehmen von transnationalen Cloud-Lösungen weiter erhöht und nun müssen diese mehr denn je eine digitale Unabhängigkeit entwickeln, um die Kontrolle über ihre eigenen Daten und die ihrer Kunden zu behalten. Denn die globalen Hyperscaler unterliegen Vorschriften, die den strategischen Interessen der Unternehmen, die sie nutzen, zuwiderlaufen können und womöglich noch eigene Gesetze verletzen. So ist beispielsweise der viel zitierte Cloud Act entstanden, der es der US-Regierung erlaubt, auf Daten zuzugreifen, die von nationalen Unternehmen gehostet werden, auch wenn sich deren Server ausserhalb der Vereinigten Staaten befinden! Folglich ist die Vertraulichkeit dieser Daten in keiner Weise gewährleistet. Angesichts der Tatsache, dass über 90 Prozent der im Westen produzierten Daten in den USA gehostet werden, stellen diese Gesetze eine Bedrohung für die Interessen der Unternehmen dar. Die digitale Souveränität gilt aber auch für den Einzelnen, wobei der Schwerpunkt auf der Wahrung des Rechts auf Privatsphäre liegt. Dies ist insbesondere dann der Fall, wenn es sich bei den den Betreibern anvertrauten Daten um sensible Daten handelt wie beispielsweise Bankdaten oder Gesundheitsinformationen.

Das Interview finden Sie auch online
www.netzwoche.ch

Was können wir dafür tun, dass die User die digitale Souveränität zurückgewinnen?

Zur Erlangung der digitalen Souveränität müssen die Schlüsseltechnologien und -kompetenzen beherrscht werden. Dabei muss die Abhängigkeit von Herstellern und der damit verbundene Vendor Lock-in gelöst werden. Ein Einzelner oder ein einzelnes Unternehmen kann nicht wirklich viel tun. Hier müssen die Länder wieder stärker das Thema in den Vordergrund rücken und die dazu notwendigen Rahmenbedingungen schaffen. Wenn wir heute im Binnenmarkt den Verkehr von Personen, Waren, Dienstleistungen und Kapital regeln, muss neu auch der Verkehr von Daten geregelt werden. Dazu gehört auch die Bereitstellung sicherer Transportwege und Speicherorte, welche die vertrauliche und sichere Übermittlung und Verarbeitung der Daten garantieren.

Wer kann dabei helfen, die digitale Souveränität wiederherzustellen?

Hier müssen Wirtschaft und Politik stärker zusammenrücken, um die dazu notwendigen Rahmenbedingungen schaffen zu können. Innovationen und Chancen technologischer Entwicklungen müssen gefördert und die rechtlichen Voraussetzungen dazu geschaffen werden. Bei der Forderung nach digitaler Souveränität sind wir nicht allein, und als Schweiz haben wir sicher

«Das Ziel ist, dass Unternehmen und User Daten sammeln und so austauschen, dass sie die Kontrolle darüber behalten.»

Martin Andenmatten, Präsident, Eurocloud Swiss

nicht das Interesse, uns vom Internet abzukoppeln. Aber hier würde ein stärkeres Zusammenarbeiten mit anderen Ländern und Interessengruppen wie beispielsweise Gaia-X, helfen, die Grundlagenarbeit dazu leisten. Hierzu fehlt es aber in der Schweiz noch am notwendigen Willen.

Welche weiteren Trends gibt es im Zusammenhang mit Daten und deren Nutzung in der Cloud?

Die Abhängigkeit von der weltweiten Technologieinfrastruktur und insbesondere von der Public Cloud wirft aktuell einige Fragen auf, ob es wirklich klug ist, die Trends und Verhaltensweisen des letzten Jahrzehnts unreflektiert fortzusetzen. Man stelle sich vor, dass eines oder mehrere der transatlantischen Kabel einem Anschlag ausgesetzt würde, wie wir dies mit der Nordstream-Pipeline miterleben mussten. Viele Unternehmen wollen ihre Abhängigkeiten reduzieren und überlegen sich genau aus diesen Gründen, ihre Cloud-First-Strategie zu überdenken und doch wieder eine Hybrid-Strategie zu fahren. Dies jedoch nicht, um alte Legacy-Systeme aufrechtzuhalten, die sich eh nur schwer in die Cloud verschieben lassen. Nein, es geht vielmehr darum, sicherzustellen, dass der Wert der wesentlichen Daten im Unternehmen belassen werden. Dabei wird man aber nicht zwischen On- und Off-Premise unterscheiden, sondern man geht von einem gemeinsamen Daten-Ökosystem aus. Die Cloud wird in Zukunft nicht, wie vielfach gedacht, nur aus den Rechenzentren der grossen Cloud-Anbieter bestehen. Vielmehr wird sich die Cloud von den Rechenzentren der Cloud-Anbieter vermehrt auch auf die Rechenzentren der Kunden und sogar deren Edge-Standorte ausweiten. Man nimmt die Konzepte der Cloud, wie Cloud-Native-Entwicklung, die Einfachheit und Skalierbarkeit der Cloud, aber man überträgt diese auf das Edge Computing. In diesem Sinne sind heute die meisten Organisationen nicht wirklich hybrid. Hybride Szenarien werden strategisch wichtige Architektur-Entscheide notwendig machen. Die verteilte Cloud ist dabei das neue Paradigma. Es geht dabei nicht primär um die Frage nach dem Hosting-Standort. Es geht vielmehr um eine Reihe von Fähigkeiten, eine neue Denkweise und ein neues Betriebsmodell.

Welche Bedeutung hat in diesem Zusammenhang das EU-Projekt Gaia-X insbesondere auch für die Schweiz?

Gaia-X ist ein von Europa initiiertes Projekt, in dem Vertreter aus Wirtschaft, Politik und Wissenschaft aus Europa und der ganzen Welt zusammenarbeiten, um eine föderierte und sichere Dateninfrastruktur zu schaffen. Das Ziel dabei ist, dass Unternehmen und User Daten sammeln und so austauschen, dass sie die Kontrolle darüber behalten. Sie sollen entscheiden, was mit ihren Daten geschieht, wo sie gespeichert werden, und stets die Datenhoheit behalten. Heute sind bereits 350 Unternehmen und Organisationen wie beispielsweise die EZB, die Europäische Zentralbank, Mitglied. Dabei gibt es verschiedenste Initiativen, wie etwa den «Sovereign Cloud Stack» (SCS) mit der Absicht, nichts weniger als eine europäische Cloud-Plattform für Unternehmen und Behörden zu entwickeln. Es sollen interoperable Cloud-Services genutzt werden, die ausschliesslich auf Open-Source-Technologien basieren und somit keine Anbieterabhängigkeit entsteht. Die verschiedenen Länder sind als Hub bei der Gaia-X eingebunden und können ihre nationalen Anforderungen einbringen und so sicherstellen. Die Schweiz wäre aus Sicht von Gaia-X sicherlich willkommen, jedoch hat sich der Bund dazu noch nicht durchringen können. Das Thema «digitale Souveränität» wird zwar diskutiert. Es fand dazu am 1. November 2022 eine Diskussionsrunde unter der Leitung von Bundespräsident Ignazio Cassis mit dem Beirat Digitale Schweiz statt. Thema war die digitale Souveränität und wie die Schweiz die Handlungsfähigkeit im digitalen Raum stärken kann. Auf den Swiss Finish wird man wohl noch länger warten müssen.

EUROCLOUD SWISS

Eurocloud Swiss ist der schweizerische Fachverband für die Förderung des Cloud Computing in der Schweiz. Mit den europäischen Partnern des Eurocloud-Netzwerks pflegt Eurocloud Swiss einen ständigen Dialog. Der Verband ist das Bindeglied in Bezug auf die europäische und globale Entwicklung im Internet-Business und die Bedürfnisse und Gegebenheiten im Schweizer Markt. Quelle: eurocloudswiss.ch

Kennen Sie Ihren aktuellen Risiko-Status?

Cyberrisiken lassen sich nie ganz vermeiden. Vielmehr müssen Unternehmen in der Lage sein, sie zu erkennen, zu priorisieren und zu managen. Wo lauern die grössten Gefahren und wie sollte man am besten vorgehen? Und welche Unterstützung können Managed Service Provider dabei bieten?

Der Autor
Richard Werner, Business Consultant, Trend Micro

«Tun Sie das nicht!» In der IT-Security hört man diesen Satz oft genug – zum Beispiel, wenn es heisst: «Verwenden Sie keine Legacy-Systeme», oder «Verzichten Sie auf die Nutzung bestimmter Schnittstellen oder Ports.» Auch wenn solche Warnungen häufig durchaus berechtigt sind, lassen sie sich in der Praxis nicht immer befolgen. Das liegt nicht etwa am mangelnden Willen der Verantwortlichen. Vielmehr erfordern die moderne Geschäftsdynamik und der harte Wettbewerb mitunter schnelle Lösungen und neue Architekturen, bei denen Sicherheitslücken auftreten können. Wollte man das vermeiden, ginge es zulasten der Agilität. Und auch, wenn jeder weiss, dass man Cloud-Services schützen muss, passieren im Eifer des Gefechts manchmal einfach Fehler. So kann jedes neue vernetzte Gerät, jeder ausgerollte Cloud-Service und jede Konfigurationsänderung eine potenzielle Sicherheitslücke darstellen. Laufend werden neue Schwachstellen veröffentlicht, und Cyberkriminelle entwickeln immer raffiniertere Angriffsmethoden.

Jedes Unternehmen hat Schwachstellen und ist angreifbar

Sicherheitsrisiken lauern oft dort, wo es hektisch zugeht oder man sie nicht sieht. In vielen Organisationen hat sich zum Beispiel eine Schatten-IT entwickelt, weil Mitarbeitende Cloud-Instanzen und Software ohne Kenntnis der IT-Abteilung nutzen. In einer dynamisch wachsenden IT-Umgebung gelingt es nicht immer, alles sauber zu dokumentieren. Meist fehlt ein zentraler Überblick. So kommt es auch vor, dass ausgemusterte Altsysteme oder verwaiste Cloud-Instanzen weiterlaufen und Schwachstellen unbemerkt bleiben.

Selbst in der Security-Abteilung passieren Fehler, etwa weil man eine Situation falsch einschätzt oder ein System nicht optimal konfiguriert hat. Es wird nie möglich sein, alle Schwachstellen zu schliessen und alle Risiken zu vermeiden. Da hilft der erhobene Zeigefinger nur wenig. Vielmehr benötigen Unternehmen eine Strategie, um ihre Risiken zu managen: Mit manchen kann man leben, mit anderen nicht. Um dies zu entscheiden, muss man die eigenen Risiken zunächst kennen und bewerten. Anschliessend kann man gezielt Massnahmen ergreifen, um die grössten Gefahren zu minimieren.

Interne und externe Quellen berücksichtigen

Um Risiken realistisch einzuschätzen, müssen Unternehmen nicht nur ihre Angriffsfläche kennen, sondern diese auch in Relation mit externen Security-Informationen betrachten. Denn nicht jedes Risiko betrifft jedes Unternehmen gleichermassen. Die berühmte Log4Shell-Schwachstelle, die vor etwa einem Jahr für Aufregung sorgte, ist zum Beispiel nur für Organisationen gefährlich, welche die Log4J-Komponente auch einsetzen.

Ausserdem hängt das Risiko, das von einer Schwachstelle ausgeht, auch immer davon ab, wie häufig Angreifer diese Sicherheitslücke gerade ausnutzen. So kann eine ältere, als wichtig eingestufte Schwachstelle aktuell gefährlicher sein als eine neue kritische, zu der Sicherheitsforscher derzeit kaum oder keine cyberkriminellen Aktivitäten verzeichnen. Je nach ihrer Grösse und Branche stehen Unternehmen zudem im Visier unterschiedlicher Hacker-Gruppen. Fällt das Unternehmen ins Beuteschema aktueller Gruppierungen und hat es Schwachstellen, die gerade häufig ausgenutzt werden? Dann ist das Risiko für einen Cyberangriff hoch.

MSPs können helfen

Das Monitoring und die Bewertung von externen Security-Quellen ist für Unternehmen jedoch fast noch schwieriger als die Analyse der Angriffsfläche. Denn täglich veröffentlichen Security-Unternehmen, Polizeiorganisationen, Regierungsbehörden, Non-Profit-Organisationen und Analysten unzählige Informationen zum cyberkriminellen Geschehen. Sie alle im Auge zu behalten und in der nötigen Detailtiefe zu verfolgen, ist für interne Teams kaum machbar. Mit einem renommierten Security-Anbieter an der Seite können MSPs ihre Kunden bei dieser Herausforderung unterstützen: Indem sie die externen Security-Informationen sammeln, analysieren und ihre Kunden proaktiv über relevante Risiken informieren, helfen sie diesen mit geringem Eigenaufwand bei der Risikobewertung.

Eine Schlüsselrolle spielt dabei Extended Detection and Response (XDR). Viele Managed Service Provider setzen diese Technologie bereits ein, um MDR-Services (Managed Detection & Response) anzubieten. XDR sammelt Informationen aller angeschlossenen Security-Systeme über alle Vektoren der IT-

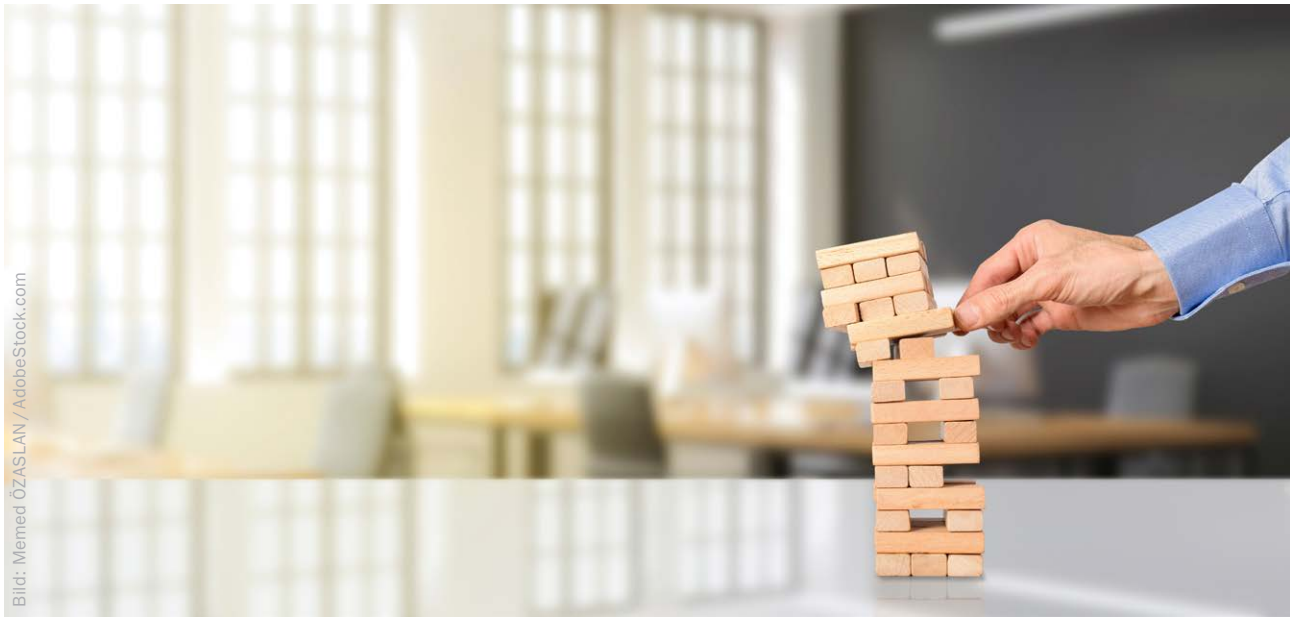


Bild: Memed ÖZASLAN / AdobeStock.com

Umgebung hinweg – von Cloud-Instanzen über Server und Netzwerke bis hinab zu Endpunkten und E-Mails. Die Daten werden KI-gestützt analysiert, die relevanten Meldungen erkannt und zu verwertbaren Warnungen korreliert, wobei globale Threat Intelligence mit berücksichtigt wird.

So gelingt aktives Cyber-Risiko-Management

XDR kann jedoch nicht nur reaktiv, sondern auch proaktiv unterstützen: Da auf der Plattform ohnehin umfassende interne und externe Security-Informationen zusammenlaufen, kann sie kontinuierlich Risiken für das Unternehmen ermitteln und bewerten. Die Daten werden übersichtlich in einem Dashboard aufbereitet, sodass MSPs auf einen Blick sehen, wo die aktuell grössten Gefahren des Kunden lauern und wo dringender Handlungsbedarf besteht. Sie können den Kunden dann proaktiv warnen und ihn dabei unterstützen, diese Risiken zu mindern. Besonders effizient wird Risikobewertung im Zusammenspiel mit Managed XDR. Spezialisierte Security-Analysten des Lösungsherstellers übernehmen dann das Monitoring und die Auswertung der Meldungen auf der XDR-Plattform. Sie entlasten die IT-Teams von Partnern und Kunden und erhöhen die Sicherheit zusätzlich, indem sie kundenübergreifende, globale Erkenntnisse und Erfahrungen mit einbringen. Ausserdem stehen sie bei Fragen mit ihrer Expertise bereit und geben Rückhalt.

XDR als Baustein für Zero Trust

Die XDR- und Threat-Intelligence-gestützte Risikobewertung ist zudem ein wichtiger Baustein für die Umsetzung einer Zero-Trust-Strategie. Diese umfasst technische und organisatorische Massnahmen, um Angriffsrisiken zu mindern. Zero Trust bedeutet: Vertraue niemandem. Durch umfangreiche interne und externe Security-Kontrollen gilt es, sicherzustellen, dass nur autorisierte Nutzer auf Systeme, Anwendungen und Daten zugreifen können. Ein umfassendes Zero-Trust-Modell umzusetzen, ist jedoch sehr aufwendig und kann Jahre dauern. In der Regel müssen Unternehmen dafür ihre Netzwerke weitreichend umstellen. XDR lässt sich dagegen in wenigen Wochen einführen und ermöglicht sowohl eine proaktive Bewertung als auch Minderung von Risiken. Die Technologie sammelt und korreliert Telemetriedaten und Warnmeldungen aller angeschlossenen Security-Systeme und analysiert sie KI-gestützt unter Berücksichtigung globaler Threat Intelligence. Dadurch können Unternehmen Zero-Trust-Massnahmen ganz gezielt dort umsetzen, wo ihre grössten Risiken liegen. Im Falle eines Cyberangriffs ermöglicht XDR zudem eine schnelle Erkennung und Reaktion.

Fazit

Cybervorfälle sind heute das grösste Geschäftsrisiko für Unternehmen weltweit. Die Bewertung und das Management von Cyberrisiken sind für sie daher unverzichtbar. Es wird immer Risiken geben, mit denen man leben muss. Entscheidend ist, die individuell grössten Gefahren zu priorisieren und dann mit gezielten Massnahmen die Eintrittswahrscheinlichkeit und den möglichen Schaden zu reduzieren. Da sich sowohl die interne als auch externe Sicherheitslage dynamisch verändert, muss Risikomanagement kontinuierlich erfolgen.

Managed Service können dabei Unterstützung bieten: Mithilfe von XDR-Technologie lässt sich Risikobewertung einfach und effizient etablieren. MSPs können diese wahlweise eigenständig oder gemanagt gemeinsam mit Security-Herstellern anbieten. Sie profitieren dabei von fundierten Analysen und sind in der Lage, Gefahren schnell zu erkennen und zu mindern. So werden sie ihrer Rolle als Trusted Advisor gerecht und helfen ihren Kunden bei der Abwehr von Cyberangriffen.

Den Beitrag finden Sie auch online
www.netzwoche.ch

«Oft sind die Grenzen zwischen Ransomware-as-a-Service-Anbieter und Affiliate fliessend»

Mit der Digitalisierung wird die Cybersicherheit in Unternehmen zu einer ernsten Herausforderung. Mathias Fuchs, Vice President Investigation & Intelligence bei Infoguard, erklärt, weshalb Unternehmen vom Angebot eines Security-Operations-Center-Providers profitieren, wie sich Cyberkriminelle organisieren und welche Gefahren er in Ransomware-as-a-Service erkennt. Interview: Tanja Mettauer

Hybride Arbeitsmodelle und die steigende Tendenz zu Homeoffice haben Cyberkriminellen neue Türen geöffnet. Weshalb sind Managed Security Services (MSS) im Bereich der Cyberabwehr notwendig und welche Vorteile bringen sie den Unternehmen?
Mathias Fuchs: Bei jedem Angriff geht es um Zeit. Je länger sich Angreifer im Netz bewegen, desto grösser ist meist der Schaden. Angriffe können zwar durch Security-Operations-Center-Monitoring (SOC) nicht verhindert, aber erkannt werden. Eine unmittelbare Unterbrechung der Angriffskette führt dazu, dass kein Schaden entsteht. Externe Security-Services haben zudem Einsicht in viele Netze und können so neue Angriffe und Angriffswellen besser erkennen und abwehren. Analystinnen und Analysten bearbeiten zudem eine grosse Anzahl an Vorfällen – im Gegensatz zu Inhouse-Teams, die zu Betriebsblindheit neigen können.

Der Fachkräftemangel im Security-Bereich veranlasst Unternehmen dazu, vermehrt auf MSS zurückzugreifen. Weshalb sollten sie in ein Security Operations Center (SOC) investieren?
Für spezialisierte Mitarbeitende ist es oft attraktiver, in einem externen Cyber Defence Center (CDC) inklusive SOC zu arbeiten. Hier bearbeiten sie eine breite Palette von Angriffen, wodurch sie schnell Erfahrung und Wissen aufbauen, aber auch Verantwortung tragen können. Entsprechend haben wir hohe Anforderungen an unsere Analystinnen und Analysten. Für ein externes CDC spricht zudem, dass fachliche Eskalationsstufen vorhanden sind. Diese sind besonders für KMUs noch schwieriger aufzubauen als die erste Verteidigungslinie. Hierfür spezialisierte Fachkräfte wie Incident Responder und Forensiker zu finden, ist extrem schwierig. In unserem CDC arbeitet etwa auch spezialisiertes Personal, das eine vergleichbare Position inhouse kategorisch ablehnt.

Welche Fähigkeiten zeichnen einen guten SOC-Provider aus? Welche Kompetenzen muss ein Provider auf jeden Fall besitzen?
Ausser einem grossen Pool an erfahrenen Mitarbeitenden ist Flexibilität zentral. Incident Response ist am Ende immer eine reaktive Aufgabe, weshalb die proaktive Vorbereitung auf einen Sicherheitsvorfall mit dem SOC-Provider enorm wichtig ist und die Bearbeitung erheblich beschleunigen kann. Dazu muss ein SOC-Provider auch über ein eigenes Computer-Security-Incident-Response-Team verfügen, denn nur so kann zeitnah interveniert werden.

Das Interview finden Sie auch online
www.netzwoche.ch

Neue Cybergefahren entwickeln sich schnell und Security-Provider müssen rasch auf neue Bedrohungen reagieren. Welche Trends sehen Sie in Bezug auf MSS im kommenden Jahr?
Ransomware-Angriffe halten uns weiterhin auf Trab, sollten für ein SOC jedoch mehrheitlich zu bewältigen sein. Durch die derzeit stark instabile geopolitische Lage kann es zudem vermehrt zu staatlichen Angriffen kommen. Speziell hier gilt es, nach den Methoden der Jäger zu arbeiten: also jagen und Fallen stellen. Sobald Angreifer Fehler machen, sitzen sie in der Falle. So können wir auch «gute» Angreifergruppen von «schlechten» unterscheiden. Die Verteidigung muss somit selbst kleinste Fehler erkennen können und gleichzeitig den Angreifern mehr Chancen geben, in die Fallen zu tappen. Diese zwei Faktoren beeinflussen die Performance eines Anbieters stark.

Welche Strategie verfolgt Infoguard, um dem allgegenwärtigen Fachkräftemangel entgegenzuwirken?
Ausser gezieltem Recruiting und der Empfehlung unserer Mitarbeitenden setzen wir vor allem auf die Personalbindung, wozu unter anderem das Aufzeigen von Entwicklungsperspektiven gehört inklusive Aus- und Weiterbildungen sowie die stetige Stärkung unseres Employer Brands und unserer Firmenkultur. Viel Wert legen wir zudem auf die Nachwuchsförderung. Wir bilden jährlich 16 Lernende aus, die in der Regel auch nach der Ausbildung bei uns bleiben.

Ein Unternehmen meldet einen Ransomware-Angriff. Wie schnell kann Infoguard auf solche Cyberattacken reagieren und wie gehen Sie konkret vor?
Schnell – normalerweise in unter einer Stunde, was wir etwa im Rahmen unseres Incident Response Retainers sogar garantieren.

Mathias Fuchs, Vice President Investigation & Intelligence, Infoguard

Wichtig zu erwähnen ist, dass üblicherweise keine SOC-Kunden von solchen Angriffen betroffen sind. Im Unterschied zu vielen anderen Anbietern sind Forensik- und Incident-Response-Untersuchungen für uns kein Selbstzweck. Dabei haben wir drei Prioritäten, um den Schaden für den Kunden so klein wie möglich zu halten. Erstens: seine Wertschöpfungskette. Ist diese unterbrochen, müssen wir gewährleisten, dass sie in einem sicheren Rahmen wiederhergestellt wird. Ist die Wertschöpfungskette intakt, wird sie nur beeinträchtigt, wenn es unvermeidlich ist und das Schadensrisiko ohne Eingriff überwiegt. Zweitens: die Abschätzung des möglichen Schadens. Hier gilt es zu verstehen, was der Angreifer gemacht hat, ob etwas verändert oder gestohlen wurde usw. Drittens: Den zukünftigen Zugang für den Angreifer erschweren – sprich, alle Zugangspunkte und Hintertüren müssen gefunden werden, um den Angreifer auszusperren. Diese Prioritäten können wir nur dann schnell und nachhaltig erfüllen, wenn Sichtbarkeit gegeben ist. Dazu nutzen wir forensische Agents, die wir den Kunden schon im ersten Call zustellen. Kleine Fälle können dadurch manchmal umgehend gelöst werden; bei grösseren dauert es selten länger als drei bis vier Wochen.

Wie definieren Sie den «Sweet Spot» einer Cyberabwehr?

Der Sweet Spot liegt im Brennpunkt von Protection, Detection und Response. Cyberabwehr darf durch User-Einschränkungen nicht mehr Schaden verursachen, als sie verhindert. Durch die Unterscheidung von Detection und Protection können wir Einschränkungen in einem der Bereiche durch Aufrüstung im anderen Bereich kompensieren. Wenn zum Beispiel aus geschäftlichen Gründen die Öffnung eines Dienstes zum Internet notwendig ist, so reduziert sich der Schutz dieses Services. Mit verbesserter Detektion kann dies jedoch kompensiert werden.

Wie organisieren sich die Akteure bei Ransomware-Angriffen und welche Bedeutung schreiben Sie Ransomware-as-a-Service (RaaS) zu?

Mit Cyberkriminalität wird mittlerweile mehr Geld umgesetzt als mit Drogen. Angreifergruppen sind hochprofessionell organisiert und spezialisieren sich zunehmend auf die einzelnen Schritte eines Angriffs. Oft sind dabei die Grenzen zwischen RaaS-Anbieter und Affiliate fliessend. Das bedeutet, dass Kriminelle RaaS zwar anbieten, die Angriffe jedoch von deren «Kunden» ausgeführt werden, welche die Anbieter wiederum am Erfolg beteiligen (Affiliate). Nicht selten treffen wir bei Verhandlungen mit den Angreifern auf sehr kompetente Ansprechpartner. Wenn die Verhandlungen aber mit einem «RaaS-Callcenter» laufen, dann sind diese meist unpersönlich und vorhersehbarer als Verhandlungen mit Angreifern direkt.

Was raten Sie Ihren Kunden, wenn es Cyberkriminelle doch geschafft haben, ihre Daten und Systeme zu verschlüsseln? Welche Verhandlungsstrategien sollten Unternehmen verfolgen? … Sollten sie überhaupt verhandeln?

Wir raten immer, mit den Angreifern Kontakt aufzunehmen, denn zu verlieren gibt es in diesem Stadium nichts. Strategien gibt es viele, müssen jedoch immer fallspezifisch angewendet werden. Seit einiger Zeit beobachten wir, dass Angreifer vermehrt Verhandlungs-Chatprotokolle veröffentlichen, weshalb Unternehmen bei der Kommunikation vorsichtig sein sollten. Daher: Von Anfang an Profis beiziehen und nicht selbst verhandeln.

Welche Trends sehen Sie für künftige Ransomware-Angriffe?

Aktuell werden Ransomware-Schäden häufig von Versicherungen getragen, was sich jedoch sicherlich ändern wird. Entsprechend müssen Angreifer den Druck erhöhen, gegenwärtig etwa, indem sie sich genauer mit den gestohlenen Daten beschäftigen. Wir haben schon Fälle bearbeitet, in denen Angreifer sauber recherchierte «Intelligence Briefs» erstellten und sehr qualifiziert erklären konnten, weshalb die Veröffentlichung der Daten für das Opfer verheerend wäre. Ein weiterer Trend sind physische Angriffe auf Infrastrukturen über OT-Netze. Dies, weil Unternehmen immer häufiger andere Strategien finden – unter anderem mit unserer Hilfe – und Lösegeldforderungen nicht bezahlen. Somit suchen Angreifer andere Wege, um ihr Geschäft voranzutreiben.

ZUR PERSON

Mathias Fuchs ist seit 2017 für Infoguard tätig und aktuell Vice President Investigation & Intelligence. Nebenberuflich ist der Österreicher seit über neun Jahren als zertifizierter SANS-Instruktor tätig und hält regelmässig auf nationalen sowie internationalen Sicherheitskonferenzen Vorträge zu den Themen Forensik und Incident Response. Des Weiteren weist er langjährige Erfahrung im Bereich Penetration Testing auf. Fuchs hält einen Master in Biomedizinischer Informatik. Quelle: Infoguard

Mercedes-Benz setzt für Digital Twins auf Microsoft Azure


Bild: Mercedes-Benz

mla. Mercedes-Benz und Microsoft wollen die Autoherstellung effizienter, widerstandsfähiger und nachhaltiger gestalten. Dies soll mit der neuen MO360 Data Platform gelingen, mit der Mercedes-Benz seine weltweit rund 30 Autofabriken mit der Microsoft-Cloud verbinden will, wie es in einer Mitteilung heisst. Damit möchte der Autohersteller Transparenz und Prognostizierbarkeit entlang der digitalen Produktions- und Lieferkettenprozesse verbessern.

MO360 basiert auf Microsoft Azure und soll Mercedes-Benz die Flexibilität und Cloud-Rechenpower bieten, um künstliche Intelligenz (KI) und Data Analytics global einzusetzen und gleichzeitig jeweils regionale Cybersicherheits- und Compliance-Standards zu erfüllen. Die Plattform sei bereits für Teams in der EMEA-Region verfügbar und werde auch in den USA und China ausgerollt, heisst es weiter.

Digitaler Zwilling der Produktion

Mit der MO360 Data Platform kann Mercedes ein virtuelles Abbild des Produktionsprozesses für seine Fahrzeuge erstellen. Dabei werden Informationen aus Montage, Produktionsplanung, Werkslogistik, Lieferkette und Qualitätsmanagement kombiniert, wie es weiter heisst. Die virtuelle Simulation und Optimierung von Prozessen vor der Umsetzung in der Fabrik helfe, die operative Effizienz zu steigern und Energieeinsparungen zu erzielen. So könnten etwa Betriebsabläufe optimiert und der CO2-Ausstoss in der Produktion verringert werden.

Die MO360 Data Platform sei die Weiterentwicklung des digitalen Produktions-Ökosystems MO360 von Mercedes-Benz, schreiben die beiden Unternehmen. Die Plattform ermögliche es, potenzielle Engpässe in der Lieferkette schneller zu erkennen und eine dynamische Priorisierung der Produktionsressourcen vorzunehmen.

Den vollständigen Artikel finden Sie online
www.netzwoche.ch

GKB migriert in Inventx-Cloud

mla. Die Graubündner Kantonalbank GKB und Inventx vertiefen ihre bereits zwölf Jahre dauernde Partnerschaft. Auch in den kommenden fünf Jahren besorgt Inventx für die GKB den IT-Betrieb und das Applikationsmanagement, die Digital Workplaces sowie Systemintegration, Security, Robotic Process Automation und Analytics, wie Inventx mitteilt.


Inventx-CEO Pascal Specht-Keller.

Während der neu vereinbarten Vertragslaufzeit will Inventx die GKB auch in ihre «ix.Cloud» migrieren. Die Cloud laufe in Inventx-eigenen Rechenzentren, garantiere Datenhaltung in der Schweiz und werde ausschliesslich hierzulande gemanagt. Ergänzend soll die Bank neu auch einzelne Services aus der «ix.OpenFinance»-Plattform beziehen. Das Migrationsprojekt soll im Herbst 2023 abgeschlossen sein.

Skalierbarkeit und Regionalität

Die Vorteile in der neuerlich vereinbarten Zusammenarbeit mit Inventx sieht GKB-CEO Daniel Fust in der Skalierbarkeit der «ix.Cloud»-Lösung und darin, dass die Bank keine «Kompromisse bei der Sicherheit oder Compliance» einzugehen habe.

Die Vertragsverlängerung freut auch Inventx-CEO Pascal Specht-Keller. «Die GKB hat an uns geglaubt, als wir mit 90 Mitarbeitenden an den Start gingen. Heute sind wir bereits mehr als 340 Spezialisten an der Schnittstelle zwischen Banking und IT», sagt Specht-Keller. «Beide sind wir anerkannte und beliebte Arbeitgeber in Graubünden, die Arbeitsplätze in der Region schaffen und in unseren jeweiligen Kerngebieten den Fokus auf Kundennutzen, persönliche Nähe und Innovation legen.»

Den vollständigen Artikel finden Sie online
www.netzwoche.ch

UBS will ihre Anwendungen in der Microsoft-Cloud betreiben

Die UBS will in den nächsten fünf Jahren mehr als die Hälfte ihrer Anwendungen in der Public Cloud betreiben. Dazu sollen auch kritische Workloads gehören. Um dieses Ziel zu erreichen, erweitert die Grossbank ihre Partnerschaft mit Microsoft Azure. Autor: Yannick Chavanne; Übersetzung: René Jaun

UBS arbeitet schon seit einiger Zeit mit Microsoft Azure zusammen. So trieb die Grossbank ihre Migration in Microsofts Public Cloud schon nach der Eröffnung der Schweizer Datenstandorte voran. Bis Anfang 2021 war bereits ein Drittel aller UBS-Anwendungen ausgelagert, wie es in einer Mitteilung heisst. Demnach wollen die beiden Unternehmen ihre Partnerschaft nun ausbauen. Ziel sei es, die Migration zu beschleunigen, sodass die Grossbank in fünf Jahren mehr als 50 Prozent ihrer Anwendungen in Microsofts Public Cloud betreibt.

«Unsere Cloud-Strategie hat unsere Arbeitsweise grundlegend verändert. Sie ermöglicht es uns, unser Technologieportfolio neu zu beleben und die Art und Weise, wie wir Anwendungen für unsere Kundinnen und Kunden entwickeln, zu überdenken», lässt sich Mike Dargan, Chief Digital and Information Officer der UBS, zitieren.

> «Unsere Cloud-Strategie hat unsere Arbeitsweise grundlegend verändert.»
>
> Mike Dargan, Chief Digital and Information Officer, UBS

Mike Dargan, Chief Digital and Information Officer, UBS.

Nachhaltigkeitsziele

Laut der Mitteilung will die UBS die Azure-Cloud auch für den Betrieb kritischer Workloads einsetzen. Ausserdem umfasse die Partnerschaft auch die gemeinsame Entwicklung von Innovationen und eine engere Zusammenarbeit in Bereichen wie der Reduzierung von CO2-Emissionen.

Letzteres gehört zu den Nachhaltigkeitszielen der UBS. Laut der Grossbank konnte sie mit dem Wechsel in die Azure-Cloud in einigen Fällen den Energieverbrauch von Workloads um bis zu 30 Prozent senken. In diesem Zusammenhang entwickelten UBS und Microsoft nach eigenen Angaben eine Open-Source-API, die Empfehlungen für die Planung von rechenintensiven Arbeitslasten gibt. Die Idee dahinter ist, darüber zu informieren, wann saubere, erneuerbare oder kohlenstoffarme Energiequellen am besten verfügbar sind.

Confidential Computing

Die «Cloud first»-Strategie von UBS werde auch durch den Einsatz von Confidential-Computing-Technologien ermöglicht, erläutern die beiden Partner. «So profitiert UBS von einer neuen Funktion zum Schutz und zur Sicherung des internen Datenaustauschs zwischen allen Abteilungen der UBS, wobei die Compliance- und Sicherheitsstandards der Bank eingehalten werden», heisst es in der Mitteilung weiter. Dadurch könne UBS nun zusätzliche Geschäftseinblicke gewinnen und neue Innovationsmöglichkeiten für ihre Kunden und Angestellten erkennen.

Im Rahmen ihrer IT-Strategie will die UBS die Rolle ihrer IT-Offshore-Standorte in Indien stärken. Laut dem CDIO soll der Fokus der dortigen Tech-Zentren auf den Themen Cloud und KI liegen. «Wir werden Rollen neu besetzen und in den nächsten ein bis zwei Jahren 7 bis 10 Managing Directors behalten, befördern und einstellen, um sicherzustellen, dass Indien eines unserer Kernzentren ist», sagte Mike Dargan gegenüber der Wirtschaftszeitung «The Economic Times».

Den vollständigen Artikel finden Sie online
www.netzwoche.ch

Wie Systemadministratoren ihre Cloud absichern (sollten)

Wer eine Cloud-Umgebung konfiguriert, darf die Sicherheit nicht ausser Acht lassen. Das IT-Sicherheitsunternehmen Scip nennt besonders häufige Konfigurationsfehler und sagt, wie sie sich vermeiden lassen. Autor: René Jaun

Den vollständigen Artikel finden Sie online
www.netzwoche.ch

Die Cloud ist eine feine Sache – aber oft auch eine gefährliche. Zumindest dann, wenn die Administratoren beim Konfigurieren der Cloud-Umgebung nicht an die Sicherheit gedacht haben. Laut Scip gibt es eine ganze Reihe von Konfigurationsfehlern, die man zu Ungunsten der Cloud-Sicherheit machen kann. In einem ausführlichen Onlinebeitrag zählt die Zürcher IT-Sicherheitsfirma «die Top 10 risikoreichsten Konfigurationen» auf. Das Unternehmen bezieht sich dabei insbesondere auf die Microsoft Cloud. Doch das Gros der genannten Punkte gilt ebenso für Cloud-Umgebungen anderer Anbieter.

Zu viele Ausnahmen, zu wenige Einschränkungen

Manche der genannten Punkte haben mit den erteilten Berechtigungen zu tun. Scip schreibt, dass sie beispielsweise bei 80 Prozent ihrer Cloud-Assessments auf mindestens ein reguläres Benutzerkonto treffen, das der globalen Administrator-Rolle zugewiesen ist. Oft gebe es auch schlicht zu viele Administratoren. Einer der häufigsten Gründe für diese Praxis sei, «dass verschiedene IT-Teams mit unabhängigen Projekten und engen Zeitplänen die Microsoft Cloud administrieren», schreibt die Firma.

Auch definierte Ausnahmen, etwa Conditional-Access-Regeln für globale Administratoren, sind Scip ein Dorn im Auge. «Leider ist die Begründung allzu oft die Umgehung von Sicherheitskontrollen oder ein Shortcut, um Zeit zu sparen», kommentiert das Unternehmen. Es rät dazu, für privilegierte Rollen nie Ausnahmen zu definieren – ausser bei Notfall-Konten (auch Breakglass-Accounts genannt), mit denen man etwa im Störungsfall noch auf die Umgebung zugreifen können sollte.

Umgekehrt werden Handlungen privilegierter Nutzer oft nicht genug eingeschränkt. Scip nennt etwa das Beispiel, dass sich Nutzer mit privilegierten Rollen von jedem beliebigen Gerät anmelden können. Das Unternehmen rät hier dazu, mittels Conditional Access festzulegen, auf welchem Gerät sich ein Benutzer mit einer bestimmten Rolle anmelden darf.

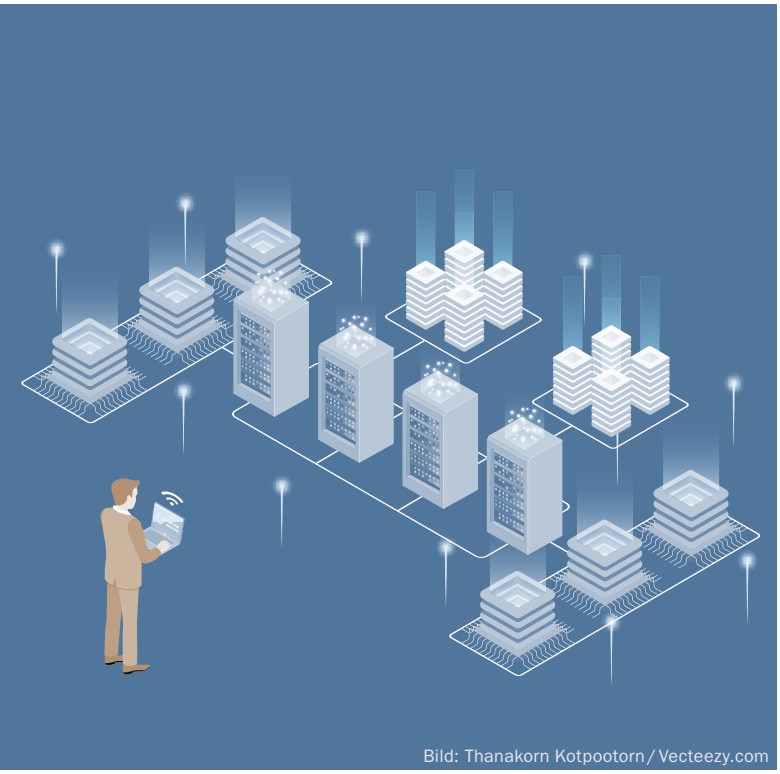


Bild: Thanakorn Kotpootorn / Vecteezy.com

Sechs Ratschläge

Konfigurationsfehler können auch aufgrund mangelnden Wissens gemacht werden. Das gehe oft Hand in Hand mit einer Silo-Mentalität, schreibt Scip. Als Beispiel nennt der Autor des Artikels vier Orte, an denen in der Microsoft Cloud Benutzerrechte verwaltet werden können. Ebenfalls gefährlich sind veraltete oder fragwürdige Denkweisen. So sei es wichtig, zu verstehen, dass der Cloud-Anbieter zwar die Tools und die Plattform für eine sichere Cloud zur Verfügung stelle. Deren Konfiguration, Überwachung und Sicherung obliege jedoch dem Kunden. «Microsoft kümmert sich schon darum», gilt also nicht.

Die sechs Schlüsselpunkte, in denen Scip den Artikel zusammenfasst, können als Ratschläge verstanden werden:

1. Vermeidung regulärer Benutzerkonten für privilegierte Aufgaben
2. Etablierung von Cloud-Identity-Access-Management-Prozessen
3. Vermeidung von zu vielen Administratoren
4. Vermeidung von Ausnahmen für privilegierte Rollen
5. Etablierung von strikten Tenant-Verwaltungsrichtlinien
6. Investition in die Denkweise eines Verteidigers und Angreifers

Die ICT-Evolution der zwei Geschwindigkeiten

Auch im Gesundheitswesen liegt die digitale Zukunft in der Cloud. Doch der Weg dahin ist anspruchsvoll. Das hat nur teilweise mit den hohen Sicherheitsanforderungen oder dem Datenschutz zu tun. Mindestens so komplex ist das Zusammenführen von Anwendungen aus verschiedenen Technologie-Generationen. Ein wichtiger Schlüssel zur Lösung dürfte dabei die hybride Cloud sein.

Kaum eine Branche hat komplexere Anforderungen an die ICT als das Gesundheitswesen. Gleichzeitig liegen die Bedürfnisse je nach Dienstleistungen oft diametral auseinander: ein Service, der «just in time» bereitgestellt wird, kann selten maximale Sicherheitsanforderungen erfüllen. Die Herausforderung besteht deshalb darin, gleichzeitig für agile und stabile Szenarien gerüstet zu sein. Denn der Trend dürfte sich in den nächsten Jahren noch verstärken: Die Bereitstellung von ICT-Diensten erfolgt zunehmend in zwei Geschwindigkeiten.

Eine Architektur für beide Welten

Ob Agilität oder Stabilität: das Serviceportfolio der Zukunft muss für beide Vorgehensweisen ausgelegt sein. Das Konzept der hybriden Cloud gewährleistet genau dies. Die «Private Cloud» integriert sicherheitskritische Dienste, darunter auch bestehende On-Premise-Applikationen. Die «Public Cloud» dagegen eignet sich für agile Projekte, die auf hoch standardisierten Umgebungen gehostet und schier endlos skaliert werden können.

Die hybride Cloud vereint somit die Vorteile beider Welten. Künftige Geschäftsprozesse im medizinischen und administrativen Kontext können in datenschutzkritische und -unkritsche Abläufe unterteilt und den passenden Umgebungen zugeordnet werden. Die private Cloud wird dabei exklusiv für Leistungserbringer im Gesundheitswesen betrieben. Die Plattformen der öffentlichen Cloud stehen allen Branchen zur Verfügung.

Benutzermanagement für das SaaS-Zeitalter

Ein wichtiger Baustein für die hybride Cloud ist die Schnittstelle am Übergang der beiden Umgebungen. Sie stellt nicht nur den Datenaustausch zwischen zwei Welten sicher. Eine wichtige Funktion ist auch der standardisierte Zugang zu den Applikationen – bis hin zur Übersicht, welches Teammitglied welchen Dienst nutzt und was für Lizenzmodelle dabei zur Anwendung kommen.

Privat oder öffentlich ist auch eine Frage der Maturität

Beim Auslagern bestehender ICT-Dienste in die Cloud muss genau hingeschaut werden. Entscheidend ist, wie sehr vorhandene Lösungen bereits als SaaS-Anwendungen konzipiert wurden, also im Kern mandantenfähig sind und so auf einfache Weise genutzt werden können. Ein Grossteil der Softwareanbieter erfüllt diese Vorgaben oft nur unzureichend.

Der Autor
Ralph Jordi, Bereichsleiter Customer Care, Hint

Daher liegt im hybriden Ansatz die Stärke für die kommenden Jahre. Sensible Patientendaten lassen sich gesetzeskonform in der privaten Cloud speichern, andere Dienste wie Anmeldeprozesse jedoch über die öffentliche Cloud realisieren. Mit allen bekannten Vorteilen wie der raschen Bereitstellung, der Skalierung, dem einfachen Abfangen von Lastspitzen oder der Abrechnung nach bezogener Leistung. Die hybride Cloud ermöglicht ICT-Dienste, die in der bestehenden On-premise-Welt nicht realisierbar sind.

Der nächste grosse Schritt der ICT im Gesundheitswesen wird also nicht ein Stichdatum sein, an dem die Migration in die Cloud abgeschlossen sein wird. Dafür sind die Anforderungen und auch die Reife der bestehenden Applikationen noch viel zu unterschiedlich. Doch ICT-Abteilungen in Spitälern oder Kliniken arbeiten bereits heute an einem neuen Szenario: an der ICT der zwei Geschwindigkeiten.

Den Beitrag finden Sie auch online
www.netzwoche.ch

Ökosystem einer modernen digitalen Kollaborations- und Kommunikationslösung

Wer mehr als nur Chat- und Meeting-Funktionalitäten nutzen will, sollte das ganze Potenzial einer Kommunikationslösung ausschöpfen – durch das Erschliessen von Synergien und den Aufbau eines darauf abgestimmten IT-Ökosystems.

Der Autor
Yannick Stauffer,
Leiter Cloud Collaboration Services,
Aveniq

Spätestens seit der Coronapandemie sind moderne Kollaborations- und Kommunikationslösungen unverzichtbarer Bestandteil des digitalen und hybriden Arbeitsalltags. Das unkomplizierte Chatten, der rasche Austausch und das gemeinsame Arbeiten an Dokumenten prägen die Arbeitskultur. Kaum ein Unternehmen konnte sich dem Trend entziehen, und so haben zahlreiche Schweizer Arbeitgeber auf Basis bestehender Infrastrukturen oder im Zuge neuer Vorhaben die digitalen Angebote im Bereich Kollaboration und Kommunikation mit entsprechenden Tools erweitert oder ganzheitlich neu geschaffen.

Trotz der immensen Möglichkeiten, die diese Plattformen beziehungsweise Tools bieten, schöpfen viele Unternehmen das Potenzial solcher Lösungen erst zu einem Bruchteil aus. Während Chat- und Meeting-Funktionalitäten relativ rasch etabliert wurden, tun sich viele Arbeitgeber schwer damit, darüber hinausgehende Möglichkeiten zeitnah zu erschliessen und diese Lösungen als integralen Bestandteil eines grösseren IT-Ökosystems zu sehen. Einerseits ist dies der Komplexität des Themas geschuldet, andererseits fehlen oftmals dedizierte Ressourcen in den Unternehmen, die sich fokussiert dieser Aufgabe annehmen können.

Synergien entlang der gesamten Wertschöpfungskette schaffen

Eine moderne Kollaborations- und Kommunikationslösung wird künftig Mittelpunkt, Ausgangspunkt sowie Schnittstelle zu Kunden, Mitarbeitenden, Lieferanten und Partnern sein. Sie geht Hand in Hand mit geeigneter Hardware, die eine hybride, moderne Arbeitsweise sowie -kultur fördert und kanalisiert eine grosse Fülle an Informationen aus den unterschiedlichsten Umsystemen. Im Idealfall starten die Mitarbeitenden zu Beginn eines Arbeitstags als Erstes die zentrale Kollaborations-/Kommunikationsplattform, egal ob am Computer, mobil via Tablet, über das Mobiltelefon oder an einem sonstigen Endgerät. Dort finden sie sämtliche Werkzeuge und Informationen in einer adäquaten Form zentral vor, die zur Erzielung erfolgreicher und effizienter Arbeitsergebnisse benötigt werden.

Diese Informationen und Arbeitsmittel können aus der kompletten Tiefe der Wertschöpfungskette eines Unternehmens entspringen: Aus umliegenden Finanz-, Logistik-, Customer-Relationship-Management-Systemen (CRM), Kundenkontaktpunkten und diversen weiteren Quellen. In geeigneter Form visuell aufbereitet, stehen sie so den Mitarbeitenden im richtigen Moment zur Verfügung. Das können zum Beispiel Einträge in der gemeinsamen Wissensdatenbank sein, die helfen, ein Problem rascher und effizienter zu lösen. Im Bereich des Kundenkontakts unterstützen Informationen, die aus dem CRM aufbereitet und mit «Predictive Analytics» angereichert sind, um Daten vorausschauend zu analysieren und mögliche Szenarien aus Datenmustern zu erkennen. Ziel ist, die Kunden so noch besser zu betreuen und zu beraten.

Die interne Zusammenarbeit lässt sich nebst den Standardfunktionalitäten mit diversen Ergänzungen verbessern. Zum Beispiel mit einem Absenzen-Manager, der ausser der Anwesenheitsübersicht Logiken wie Freigabeprozesse und Stellvertreterregelungen beinhaltet. Im Bereich der Telefonie lassen sich Anrufe mithilfe von hinterlegten Skill-Regeln zielgerichteter den passenden Personen zuteilen oder weiterleiten. Mitarbeitende sollen überall, wo sinnvoll, Zugriff auf hilfreiche produktions- und managementbezogene Echtzeitdaten erhalten und somit in der Lage sein, rascher und unabhängiger die richtigen Entscheidungen zu treffen.

Dass die Technologie und die Daten demokratisiert und zur gemeinsamen Sache werden, ist eines der Hauptziele eines IT-Ökosystems, das sich um eine Kollaborations- und Kommunikationsplattform aufbaut. Das ist auch nach der initialen Einführung ein wichtiger Bestandteil eines fortwährenden, nachhaltigen Optimierungsprozesses. Ein solches IT-Ökosystem muss nicht zwingend in einem Zug im Rahmen eines Grossprojekts umgesetzt werden. Ausgehend vom Kern der Kollaborations- oder Kommunikationslösung kann ein umliegendes Ökosystem schrittweise ergänzt und optimiert werden.

Konzeption und Schulung als Schlüssel zum Erfolg

Basis für den Erfolg einer digitalen Kollaborations- und Kommunikationsplattform inklusive des umliegenden, befähigenden

Bild: elenabs / iStock.com

IT-Ökosystems ist die konzeptionelle Arbeit. Involvieren Sie möglichst früh alle relevanten internen und externen Anspruchsgruppen, um die technologischen Grundlagen zu erarbeiten, den Zuspruch der Organisation und der Geschäftsleitung zum Vorhaben abzuholen und einen Fahrplan aufzustellen, der die Mitarbeitenden nach einem Rollout sorgfältig an die neuen technologischen Möglichkeiten heranführt.

Das beste digitale Ökosystem bringt nicht die erhofften Mehrwerte, wenn die Mitarbeitenden nicht wissen, wie dieses effizient zu bedienen ist oder deren Inhalt und der konzeptionelle Grundaufbau am gewünschten Nutzen vorbeizielt. Ein Teil des Konzepts widmet sich explizit der Schulung und der technologischen sowie kulturellen Adoption unterschiedlicher Zielgruppen. Dazu gehören nicht nur interne Mitarbeitende mit PC-Arbeitsplatz. Eine elementare Zielgruppe sind in vielen Branchen auch die wichtigen Mitarbeitenden an der Front, die sogenannten «Blue Collar Workers», die in die digitale Arbeitswelt einzubinden sind und eine wichtige Komponente eines gut funktionierenden IT-Ökosystems im Umfeld von Kollaboration und Kommunikation darstellen.

Zur Förderung des Adoptions- und Schulungsvorhabens hat sich die Ausbildung von digitalen Champions bewährt. Freiwillige Mitarbeitende, aus den unterschiedlichsten Fachbereichen rekrutiert, werden nach dem «Train-the-Trainer»-Prinzip ausgebildet und tragen das Wissen zielgerichtet und adressatengerecht ins Unternehmen.

Boxenstopp vor der Weiterentwicklung

Obwohl die konzeptionellen Grundlagen bestenfalls so früh wie möglich zu erarbeiten sind, so ist es dafür auch nie zu spät. Wie eingangs erwähnt, haben viele Unternehmen bereits seit einiger Zeit entsprechende Kollaborations- und Kommunikationsplattformen im Einsatz, deren Einführung unter Umständen auch aufgrund externer Faktoren stark beschleunigt werden musste. Spätestens aber bevor diese Plattformen weiterentwickelt und neue Umsysteme angeschafft werden, ist es ratsam, sich die Zeit für die Erstellung dieser wichtigen Grundlagen zu nehmen.

Es gilt, neue Komplexität in der Systemlandschaft zu vermeiden und bestehende zu reduzieren. Mitarbeitende sehen sich oft mit einer Fülle von Tools und nicht aufbereiteten, auf verschiedenen Plattformen zerstückelten Informationen konfrontiert. Die Gefahr besteht, dass die Belegschaft die Übersicht verliert und in der Folge an Effizienz einbüsst. Mit einem durchdachten Kollaborations- und Kommunikations-Ökosystem stellt man sicher, dass Systeme und Prozesse nahtlos ineinandergreifen und Mehrwerte sowie Synergien innerhalb des ganzen Unternehmens erzielt werden.

Unterstützung durch einen passenden IT-Partner

Nicht jedes Unternehmen verfügt über die nötigen Kompetenzen oder Ressourcen, um ein komplexes und integriertes IT-Ökosystem zu konzeptionieren und umzusetzen. In solchen Fällen bietet sich die Zusammenarbeit mit einem technologisch vielseitig aufgestellten und erfahrenen IT-Partner an. Die Begleitung durch den gesamten Prozess und die gemeinsame Erarbeitung einer massgeschneiderten, durchgängigen und sicheren Lösung spart Zeit, schont die Ressourcen und bringt Inspiration anhand von Umsetzungsbeispielen aus unterschiedlichen Branchen.

Den Beitrag finden Sie auch online
www.netzwoche.ch

Multi-Cloud-Komplexität erkennen und in den Griff bekommen

Hybride Cloud-Landschaften sind dank Flexibilität, Sicherheit und Skalierbarkeit attraktiv für Unternehmen. Doch nur die wenigsten verfügen über die Strategien, Werkzeuge, Ressourcen oder Prozesse dafür. Konnektivitätsplattformen schaffen Abhilfe.

Hybride Infrastrukturen bieten Flexibilität, Agilität, Individualität und Sicherheit – von privaten Umgebungen bis zur unbegrenzten Skalierbarkeit der Public Cloud. Oft sind aber die Systeme untereinander wenig synchronisiert, was den Datenaustausch oder die Digitalisierungsvorhaben bremst. Mit Multi-Cloud-Konnektivitäts-Plattformen sind solche Fallstricke lösbar.

Der Autor
Frank Schumacher, Head of Sales, T-Systems Schweiz

Mit den Vorteilen kommen auch Herausforderungen

In einer hybriden Umgebung kommt gleichzeitig eine Vielzahl an Technologien, Softwarelösungen und Cloud-Services zur Anwendung, deren Betrieb viele Ressourcen beansprucht. Die unterschiedlichen Betriebsmodelle lassen sich oft nicht intuitiv managen. Die fehlende Interoperabilität erschwert eine nahtlose Cloud-Migration wie auch die anschliessende Integration von On-Premises-, Private- und Public-Cloud-Umgebungen. Zudem sind Fachkräfte rar, die mit einem solchen Mix an Landschaften umgehen können. Sind ausserdem noch Legacy-Systeme im Einsatz, erhöht sich der Mehraufwand für das IT-Management weiter. Passende Schnittstellen sind für einen Datenaustausch in komplexen Umgebungen deshalb zentral, zumal Datenschutzbestimmungen wie die DSG sowie Vorgaben für besonders regulierte Branchen ebenso abgebildet sein müssen.

Externe Plattformen für die Verwaltung einer hybriden Infrastruktur

Um diese Komplexität in den Griff zu bekommen, stellen externe IT-Anbieter Multi-Cloud-Connectivity-Plattformen (MCCP) für hybride IT-Systeme zur Verfügung. Diese gemanagten Plattformen verbinden die sichere Private Cloud mit all ihren Vorteilen und dem «Look & Feel» einer Public Cloud. Welche Workloads cloudbasiert oder klassisch ablaufen, kann individuell bestimmt werden; die Plattform gewährt die notwendige Flexibilität. Jedes Unternehmen kann entscheiden, ob das eigene Rechenzentrum oder ein externes genutzt werden soll. Entsprechend wird der IT-Betrieb in diesem As-a-Service-Modell für das Unternehmen vereinfacht, beschleunigt und kosteneffizient nach Ressourcenkonsum abgerechnet.

Komplexität reduzieren und Prozesse automatisieren

Gemanagte Plattformen sorgen dafür, dass die Prozesse zwischen den einzelnen Clouds reibungslos ineinandergreifen, wobei sich Applikationen sicher verschieben, Ressourcen zuweisen oder wieder entfernen lassen. In einer Multi-Cloud-Connectivity-Plattform läuft das automatisiert ab. Das System wird agiler, die Integration der Applikationen gestaltet sich einfacher und die OPEX sinkt.

Ein hoher Automatisierungsgrad reduziert allgemein Risiken und ist weniger fehleranfällig. Zudem lassen sich Workloads vereinheitlichen und jederzeit um Public-Cloud-Services ausbauen. Auch die Reaktionsfähigkeit steigt: Benötigt ein Ressort für den Test neuer Services schnell eine Entwicklungsumgebung, lassen sich Multi-Cloud-Connectivity-Plattformen innerhalb kurzer Zeit hunderte virtuelle Maschinen zur Verfügung stellen.

Nicht zuletzt können Unternehmen dank einer Konnektivitätsplattform Rechtssicherheit gewährleisten. Der Zugriff auf die Plattform ist jederzeit möglich, um etwa eigene Compliance-Reports und Audits zu erstellen.

Kosteneffizient arbeiten (lassen)

Mit der richtigen Infrastruktur lassen sich unterschiedlichste Applikationen in beliebigen Rechenzentren performant als Managed Service betreiben. «Lift and Shifts» sind einfacher umzusetzen, hohe Migrationskosten und aufwendige Neuinstallationen entfallen. Schliesslich lassen sich in hybriden Umgebungen auch Angebote von Hyperscalern punktuell und flexibel hinzubuchen. Alles in allem bieten Multi-Cloud-Konnektivitätsplattformen das Beste aus allen IT-Welten in einer.

Bild: thodonal / AdobeStock.com

«Mit der MCCP kann ein ‹leastcost routing› durchgeführt werden»

Will ein Unternehmen über verschiedene Clouds hinweg für Compliance, Sicherheit und Verfügbarkeit sorgen, bietet sich eine Multi-Cloud-Connectivity-Plattform an. Im Interview sagt Thorsten Bolz, Vice President Cloud Services bei T-Systems, wann und für wen sich eine solche Plattform lohnt. Interview: René Jaun

Thorsten Bolz, Vice President Cloud Services, T-Systems.

Wann ist für ein Unternehmen der Zeitpunkt gekommen, eine Multi-Cloud-Connectivity-Plattform (MCCP) einzuführen?
Mithilfe der MCCP haben Unternehmen die Möglichkeit, schnell und auf Knopfdruck eine Layer-3-IP-Verbindung herzustellen. Die MCCP ergibt vor allem dann Sinn, wenn ein Unternehmen seine Flexibilität in der Bereitstellung von Workloads in unterschiedlichen Landingzones – sowohl in Private- wie auch Public-Umgebungen – erhöhen will beziehungsweise muss. Unternehmen können so bedarfsgerecht Verbindungen auf- und abbauen, etwa wenn sie rasch eine Test- oder Entwicklungsplattform benötigen. Beispielsweise kann die Produktivumgebung auf AWS laufen und parallel eine Testumgebung auf Azure aufgesetzt werden. Mittels der MCCP kann diese Verbindung temporär etabliert werden. Nach dem Deployment der Testsysteme wird sie umgehend wieder heruntergefahren.

Wann lohnen sich solche Plattformen für KMUs?
Unternehmen, die bereits den Nutzen einer Multi-Cloud-Strategie erkannt haben, stehen vor der Herausforderung, über die verschiedenen Clouds hinweg für Compliance, Sicherheit und Verfügbarkeit zu sorgen – und die Kosten dafür im Griff zu behalten. Für sie ist die MCCP die geeignete Wahl, alle Cloud-Dienste nahtlos über eine einzige Netzwerkplattform zu bündeln und zu managen. Damit sparen sie und beschleunigen gleichzeitig ihre Digitalisierung, denn sie können sich viel flexibler und hochautomatisiert beim Auf- und Abbau von Verbindungen über unterschiedliche Landingzonen hinweg bewegen und damit die beste Funktionalität für jeden Workload auswählen.

Wie bereitet ein IT-Team die Einführung einer MCCP vor?
Die Einführung einer MCCP in einem Unternehmen ist immer ein gemeinschaftlicher Ansatz zwischen T-Systems und dem Unternehmen. T-Systems führt in der Regel immer mehrere Workshops mit dem Kunden durch, um die Netzwerk-Parameter auf beiden Seiten festzulegen. Hier ist es wichtig, dass der Kunde Transparenz hat über seine bestehende Netzwerkinfrastruktur, seine Netzwerktopologie ganzheitlich versteht und sie – so weit notwendig – offenlegen kann.

Was ist nach der Einführung zu tun, um mit einer MCCP auch wirklich Kosten sparen zu können?
Mit der MCCP kann letztlich ein «leastcost routing» durchgeführt werden, das heisst, die Unternehmen, welche die MCCP nutzen, müssen dafür Sorge tragen, dass der Service dort genutzt wird, wo man das beste Verhältnis Kosten vs. Sicherheit und Nutzen hat. Wir können dabei unterstützen, die bestmögliche Zielplattform für die jeweiligen Workloads zu definieren.

Wie stellt eine MCCP den Schutz sensibler Unternehmensdaten sicher?
Die MCCP ist mit einer Konnektivitätsschicht ausgerüstet, die das Multi-Cloud-Ökosystem mit Ende-zu-Ende-Sicherheit und Compliance verbindet. Kundenspezifische Cloud-Routing-Domänen sichern die IP-Datenverkehrsströme zum Schutz der Daten. Ausserdem unterliegt die MCCP-Plattform dem ESARIS-Sicherheitsstandard und wird somit regelmässig auditiert. Damit wird ein höchstmöglicher Schutz aller Daten sichergestellt.

Das Dossier finden Sie auch online
www.netzwoche.ch

Bechtle bietet Multi-Cloud-as-a-Service

cka. Das deutsche IT-Systemhaus Bechtle will Unternehmen den Weg in die Multi-Cloud vereinfachen. Zu diesem Zweck lanciert Bechtle einheitliche Cloud Operation Services für die Hyperscale-Cloud-Plattformen Amazon Web Services (AWS), Microsoft Azure und Google Cloud, wie das Systemhaus mitteilt.

Dabei handelt es sich um ein identisches, vollumfängliches Modell zur Nutzung der drei führenden Hyperscale-Cloud-Provider. Dies deckt Beratung, Konfiguration, Onboarding und den gesamten Nutzungszyklus ab – einschliesslich kontinuierlicher Kosten- und Governance-Optimierungen für einen dauerhaft effizienten Betrieb.

Bestellung und Abrechnung erfolgen über Bechtles Cloud-Marktplatz. Die Abrechnung richtet sich laut Mitteilung nach dem Verbrauch. Wer keine Multi-Cloud-Umgebung wünscht, kann auch die Dienste eines einzelnen Providers beziehen. Das Angebot soll vor allem KMUs Optionen für eine schnelle, cloudbasierte IT-Transformation bieten. So müssten sie nicht zusätzlich in Fachpersonal und entsprechendes Know-how investieren.

Den vollständigen Artikel finden Sie online
www.netzwoche.ch

Fujitsu kündigt Computing-as-a-Service an

pwo. Fujitsu drängt ins Geschäft mit Computing-as-a-Service (CaaS). Kunden des japanischen Herstellers erhalten Zugang zu Computing-Technologien über die öffentliche Cloud, darunter zu einem Computer, der mit demselben Prozessor wie der Supercomputer Fugaku ausgestattet ist. Bisher waren diese Rechentechnologien weitgehend auf Anwendungen im akademischen Umfeld beschränkt, wie Fujitsu mitteilt. Der Service startete im Oktober 2022 in Japan. 2023 soll das Angebot weltweit zur Verfügung stehen.

«CaaS wird den Kunden einen nahtlosen Zugang zu Services in der Public Cloud bieten, um die schnell wachsenden Anforderungen an das Computing zu erfüllen und die weltweit führenden fortschrittlichen Computing-Technologien von Fujitsu zu nutzen», sagt Vivek Mahajan, Chief Technology Officer von Fujitsu. «In Zukunft wollen wir das Portfolio mit Technologien wie Quantencomputing weiter ausbauen.» Zunächst starte man mit Vorbestellungen für den Cloud-Service HPC, der die Rechenleistung des Supercomputers Primehpc FX 1000 biete.

Den vollständigen Artikel finden Sie online
www.netzwoche.ch

PaaS-Geschäft boomt in Europa

aob. Die Ausgaben für Public-Cloud-Dienste sollen 2022 in Europa 113 Milliarden US-Dollar erreichen. Das entspricht einem Wachstum von 26,4 Prozent gegenüber dem Vorjahr. Bis 2026 soll sich dieser Betrag bei einer durchschnittlichen jährlichen Wachstumsrate von 22 Prozent über fünf Jahre auf 239 Milliarden US-Dollar mehr als verdoppeln. Dies prognostizieren die Marktforscher von IDC im «Worldwide Public Cloud Services Spending Guide».

Bild: Maksim Kabakou / Fotolia.com

Den grössten Teil der Ausgaben in Public Clouds machen auch 2022 Investitionen in Software-as-a-Service (SaaS) aus, wie IDC weiter schreibt. Das am schnellsten wachsende Marktsegment sei aber Platform-as-a-Service (PaaS).

Bis zu 60 Prozent dieser Investitionen gehen gemäss IDC auf das Konto von Dienstleistern, die Bankenbranche und die Fertigungsindustrie. Die Umsetzung von Digital-First- und cloudbasierten Strategien stehe weiterhin zuoberst auf den Agenden von IT-Entscheiderinnen und -Entscheidern.

«Europäische Unternehmen wollen ihre Prozesse automatisieren, da sie mit den Herausforderungen des Marktes konfrontiert sind, darunter Unterbrechungen der Lieferkette und Fachkräftemangel», sagt Andrea Minonne, Senior Research Analyst bei IDC. «Immer häufiger werden Unternehmen die Cloud nutzen, um eine solide Grundlage für die Datenanalyse in Echtzeit zu schaffen, die schliesslich die Agilität und Widerstandsfähigkeit des Unternehmens unterstützt.»

Den vollständigen Artikel finden Sie online
www.netzwoche.ch

Cloud-Services-Markt fördert regionale Angebote – auch die von Hyperscalern

Der weltweite Markt für Cloud-Services ist im vergangenen Jahr stark gewachsen. Regionale Anforderungen führen zu guten Geschäftsmöglichkeiten für lokale Anbieter. Davon können allerdings auch Hyperscaler profitieren, wie etwa Microsofts Azure-Cloud in der Schweiz zeigt. Autor: Coen Kaat

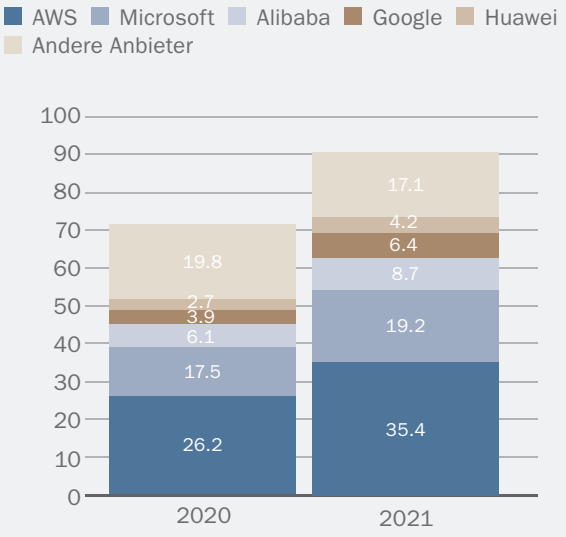
Der Markt für Public-Cloud-Angebote im Bereich Infrastructure-as-a-Service (IaaS) ist im vergangenen Jahr ordentlich gewachsen. Im Jahresvergleich steigerte sich der Umsatz um 41,4 Prozent, wie Marktforscher Gartner festhält. 2021 kletterte der weltweite Umsatz von 64 Milliarden US-Dollar auf 90,9 Milliarden. «Der IaaS-Markt wächst unvermindert weiter, da Cloud-Native zur primären Architektur für moderne Workloads wird», sagt Sid Nag, Analyst bei Gartner. «Die Cloud unterstützt die Skalierbarkeit und Kompositionsfähigkeit, die fortschrittliche Technologien und Anwendungen erfordern, und ermöglicht es Unternehmen gleichzeitig, neue Anforderungen wie Datensouveränität, Datenintegration und eine verbesserte Kundenerfahrung zu erfüllen.»

Schlüsselt man den Markt nach Anbietern auf, sieht man, dass einige 2021 deutlich mehr beigetragen haben als andere. Gartner schreibt, dass die Top 5 der Anbieter 80 Prozent des Marktes ausmachen. Diese Aussage stimmt zwar, doch verfälscht sie das Bild auch ein wenig: der Branchenprimus allein deckt nämlich bereits fast 40 Prozent des Marktes ab und steht (aktuell) quasi ausser Konkurrenz. Dabei handelt es sich um Amazon Web Services (AWS). Mit einem Umsatz von 35,4 Milliarden Dollar sicherte sich das Unternehmen einen Marktanteil von 38,9 Prozent. Im Vergleich zum Vorjahr musste AWS jedoch (trotz Umsatzwachstums) einen Teil seines Kuchenstücks einbüssen: 2020 hatte das Unternehmen noch einen Marktanteil von 40,8 Prozent.

An zweiter Stelle folgt Microsoft – allerdings mit einem klaren Abstand. Der Azure-Anbieter erwirtschaftete im vergangenen Jahr fast 19,2 Milliarden Dollar – eine Steigerung von 51,3 Prozent. Damit sicherte sich das Unternehmen einen Marktanteil von 21,1 Prozent. Im Gegensatz zu AWS baute Microsoft seine Marktpräsenz aus. Im Vorjahr machte Microsoft noch 19,7 Prozent des Gesamtmarktes aus. Viele Unternehmen setzen bereits auf Business-Software von Microsoft. Somit ist Azure gemäss Gartner in einer guten Position, um Geschäftsmöglichkeiten in fast allen vertikalen Märkten zu ergreifen.

Der Marktanteil der Gruppe der «weiteren Hersteller» sinkt zwar auf 18,8 Prozent. Dennoch betont Gartner in seiner Analyse die steigende Bedeutung von regionalen Angeboten. «Regionale Cloud-Ökosysteme werden angesichts der zunehmenden geopolitischen Fragmentierung sowie neuen regulatorischen und Compliance-Anforderungen immer wichtiger und stellen eine Chance für Anbieter mit einer starken regionalen Präsenz dar», sagt Nag.

DER GLOBALE MARKT FÜR IAAS-ANGEBOTE AUS DER PUBLIC CLOUD 2020 VS. 2021



Quelle: Gartner

Der Hyperscaler aus der Region

Von dieser Regionalität profitieren nicht nur lokale Anbieter, wie eine aktuelle Studie von ISG zeigt. Schweizer Unternehmen – obwohl traditionell eher vorsichtig bei der Cloud-Migration – würden mittlerweile häufiger auf Microsofts Azure-Cloud setzen. Dies führt der Marktforscher darauf zurück, dass die Schweiz seit 2020 eine eigenständige Region bei der Bereitstellung von Azure-Diensten ist. Seit der Veröffentlichung der ISG-Studie kündigte das Unternehmen zudem Azure-Verfügbarkeitszonen in der Schweiz an. Innerhalb der Region Switzerland North werden Instanzen repliziert, was die Ausfallsicherheit erhöhen soll.

«Azure erobert Schritt für Schritt einen festen Platz im Schweizer Cloud-Geschäft», sagt Uwe Ladig, Director bei ISG im DACH-Raum. «Viele hiesige Unternehmen migrieren zu Azure, indem sie mit Serviceanbietern zusammenarbeiten, die über lokale Niederlassungen verfügen und welche die gestellten Sicherheitsanforderungen erfüllen.»

Den vollständigen Artikel finden Sie online
www.netzwoche.ch

Kanton Zürich hält Verträge zu Microsoft 365 geheim

Der Zürcher Regierungsrat hat den Einsatz von Microsoft 365 in der kantonalen Verwaltung bewilligt. Doch wer sich für die vertraglichen Grundlagen dieser Zulassung interessiert, guckt in die Röhre. Das sorgt für Kritik. Autor: René Jaun

Die Verwaltung des Kantons Zürich darf den Cloud-Dienst Microsoft 365 nutzen. Dies hatte der Regierungsrat im April 2022 entschieden. Der Beschluss gilt für sämtliche der kantonalen IKT-Strategie unterstehenden Behörden sowie die Kantonspolizei. Im Vergleich zu einer On-Premise-Lösung sei das IT-Sicherheits- und Datenschutzrisiko der Microsoft-Cloud nicht höher. Das Risikoprofil sei jedoch anders, befand der Rat.

Verträge bleiben geheim

Das Vertragswerk zwischen dem Kanton Zürich und Microsoft wurde mit einer von der kantonalen Datenschutzbeauftragten gestützten Ergänzung abgeschlossen. Doch was konkret in diesem Vertrag steht, will der Kanton nicht sagen, wie aus einem Blogbeitrag von Rechtsanwalt Martin Steiger hervorgeht. Darin beschreibt er seine weitgehend fruchtlosen Bemühungen, gestützt auf das Öffentlichkeitsprinzip Zugang zu den Dokumenten zu erhalten.

Steiger scheiterte sowohl bei der Zürcher Datenschutzbeauftragten als auch beim kantonalen Amt für Informatik. Von Ersterer erhielt der Anwalt lediglich eine Bestätigung, «dass der (nun auf Deutsch übersetzte) Wortlaut dem entspricht, was Microsoft im Rahmen der von uns begleiteten Verhandlungen zugesicherte hatte». Den eigentlichen Vertragszusatz lieferte die Datenschutzbeauftragte indes nicht – mit Hinweis auf die Schweigepflicht.

Den vollständigen Artikel finden Sie online
www.netzwoche.ch

Auf diese beruft sich auch das Amt für Informatik: «Das Vertragswerk zwischen dem Kanton Zürich und Microsoft sieht ausdrücklich vor, dass die zwischen den Parteien geschlossenen vertraglichen Bestimmungen vertraulich sind und dass beide Personen sich verpflichten, diese vertraulichen Informationen Dritten gegenüber nicht offenzulegen», zitiert Steiger aus dem ablehnenden Bescheid. Darin heisst es weiter, es gebe ein «überwiegendes öffentliches Interesse des Kantons Zürich an der Einhaltung eingegangener vertraglicher Pflichten, damit der Kanton Zürich als zuverlässiger Vertragspartner anerkannt bleibt und damit die Allgemeinheit nicht für die finanziellen Folgen eines Vertragsbruches einstehen muss».

Bild: fergregory / AdobeStock.com

Keine Vorbildwirkung

«Der Kanton Zürich hat das Vertragswerk mit Microsoft demnach mit Wissen und Willen dem Öffentlichkeitsprinzip entzogen, anstatt den Grundsatz der Öffentlichkeit im Vertragswerk zu berücksichtigen», kritisiert Steiger. Mit der Geheimhaltung gefährden die Behörden das Vertrauen der Bürgerinnen und Bürger. Zudem habe der Regierungsratsentscheid auch keine Vorbildwirkung mehr. Eine solche wäre nur vorhanden, «wenn die Grundlagen dieser Zulassung öffentlich zugänglich wären und unabhängig überprüft werden könnten».

Microsoft verzichtet auf Anfrage auf eine Stellungnahme: «Wir äussern uns grundsätzlich nicht zu vertraglichen Bestimmungen zwischen unseren Kunden oder Partnern und uns», schreibt das Unternehmen.

Während die Zürcher Datenschutzbeauftragte den Microsoft-Vertrag absegnete, riet der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) in einem anderen Fall zum Verzicht. Dabei beurteilte er die Pläne der Suva, ebenfalls in die Microsoft-Cloud zu wechseln. Den EDÖB ging es vor allem um den theoretisch möglichen Zugriff auf Daten in einem Schweizer Microsoft-Rechenzentrum durch den US-Mutterkonzern im Rahmen des Cloud-Acts.

Markt für IT- und Business-Services weiterhin robust

Der Markt für IT- und Business-Services hat laut ISG-Index gegenüber Vorjahr um 18 Prozent zugelegt. Managed Services bleiben auf Wachstumskurs. Die Dynamik bei cloudbasierten XaaS schwächelte hingegen. Autor: Marc Landis

Bild: Freepik Company S.L. / freepik.com

Der europäische Markt für IT- und Business-Services hat im zweiten Quartal 2022 im Vergleich zum Vorjahr ein deutliches Wachstum gezeigt. Doch vor dem Hintergrund zunehmender wirtschaftlicher Unruhe gab es auch Zeichen einer sich abschwächenden Marktdynamik, wie dem aktuellen EMEA-ISG-Index der Information Services Group zu entnehmen ist.

Der EMEA-ISG-Index erfasst Fremdvergaben mit einem jährlichen Vertragswert (Annual Contract Value, ACV) von mindestens 5 Millionen US-Dollar. Der ACV des Gesamtmarktes aus Managed Services und cloudbasierten XaaS überschritt mit 7,6 Milliarden Dollar demnach zum dritten Mal in Folge den Quartalswert von 7 Milliarden Dollar. Dies entspricht einem Plus von 18 Prozent gegenüber dem entsprechenden Vorjahresquartal, wie ISG vorrechnet.

XaaS

Im zweiten Quartal überstieg die Nachfrage nach XaaS in EMEA das vierte Quartal in Folge die Marke von 3,5 Milliarden Dollar und erreichte 3,8 Milliarden Dollar. Wie ISG weiter schreibt, entspricht dies einem Wachstum von 27 Prozent gegenüber dem entsprechenden Vorjahresquartal, aber auch einem Rückgang von 3 Prozent gegenüber dem ersten Quartal 2022.

Innerhalb dieses Marktsegments legten Infrastructure-as-a-Service (IaaS) im Jahresvergleich um 30 Prozent auf 2,8 Milliarden US-Dollar und Software-as-a-Service (SaaS) um 19 Prozent auf 962 Millionen US-Dollar zu, wie ISG weiss. Mit Blick auf das Vorquartal hingegen lag das Minus demnach bei 3 Prozent beziehungsweise 4 Prozent.

Das Auftragsvolumen im Teilmarkt der Managed Services setzte seinen Wachstumstrend fort und erreichte 3,9 Milliarden US-Dollar und damit 10 Prozent mehr als im gleichen Quartal des Vorjahres und 3 Prozent mehr als im ersten Quartal 2022. Zum fünften Mal in den vergangenen sieben Quartalen lag hier der ACV über 3,5 Milliarden Dollar, wie es weiter heisst. Dabei lag das IT-Outsourcing (ITO) mit 2,9 Milliarden Dollar 1 Prozent über dem Vorjahreswert und 4 Prozent über dem Wert des ersten Quartals.

Besonders stark war die Nachfrage nach Services laut ISG bei der Anwendungsentwicklung und -wartung (ADM), die gegenüber dem Vorjahr um 17 Prozent und gegenüber dem ersten Quartal 2022 um 29 Prozent zulegten. Der Umsatz im Bereich Business Process Outsourcing (BPO) wuchs dank branchenspezifischer Services um 47 Prozent auf 968 Millionen Dollar, ging aber im Vergleich zum Vorquartal um 1 Prozent zurück, wie es im ISG-Index weiter heisst.

Managed Services in DACH rückläufig

Mit Blick auf die einzelnen Länder wiesen Benelux, Frankreich und Südeuropa im Jahresvergleich ein zweistelliges Wachstum bei den Managed Services auf, während dieser Markt in Deutschland, Österreich und der Schweiz (DACH) sowie in den nordischen Ländern rückläufig war. Wie im ISG-Index zu lesen ist, wies das Vereinigte Königreich ebenfalls ein Minus auf, erwirtschaftete aber dennoch im dritten Quartal in Folge einen ACV von mehr als 1 Milliarde US-Dollar. Dieses Niveau erreichte der Markt seit dem Brexit bislang nur ein Mal im Jahr. Doch nun ist in Grossbritannien ein nachhaltigeres Level bei den Vertragsabschlüssen zu beobachten.

Der Gesamtmarkt in Europa erreichte in der ersten Jahreshälfte 2022 einen ACV-Rekordwert von 15,2 Milliarden Dollar und damit 20 Prozent mehr als im gleichen Zeitraum des Vorjahrs. XaaS wuchsen um 35 Prozent auf ein neues Hoch von 7,6 Milliarden Dollar, was etwas mehr als 50 Prozent des Gesamtmarktes entspricht.

Angesichts der anhaltenden wirtschaftlichen Unsicherheiten hat ISG seine globale Prognose für XaaS (IaaS und SaaS) von im letzten Quartal noch 22 Prozent auf nun 18 Prozent Wachstum für das gesamte Jahr 2022 revidiert. Die globale Wachstumsprognose für Managed Services stufte ISG von 5,1 Prozent auf 3,5 Prozent herab.

Den vollständigen Artikel finden Sie online
www.netzwoche.ch

Eine kleine Geschichte der Cloud

Die Cloud ist aus der heutigen Businesswelt nicht mehr wegzudenken. Unternehmen wie AWS, Google und Microsoft haben deren Entwicklung massgeblich geprägt. Das erste System, das heute als «Cloud» bezeichnet würde, stammt aber von einer anderen Firma. Autor: Kevin Fischer

1995

Das Forschungszentrum **GMD** (heute Fraunhofer FIT) stellt mit dem BSCW (Basic Support for Cooperative Work) ein System vor, das heute als Cloud bezeichnet werden würde. User konnten webbasierte Dokumente in Ordner hochladen und mit anderen teilen.

2006

AWS startet im März Amazon S3 (Amazon Simple Storage Service), ein frühes Infrastructure-as-a-Service-Angebot (IaaS). Im August desselben Jahres lanciert das Unternehmen die Amazon Elastic Compute Cloud (Amazon EC2). Darauf konnten User Daten speichern und neu auch verarbeiten.

2008

Google kündigt seinen ersten Cloud-Computing-Service an: App Engine, eine Plattform, um Webapplikationen zu entwickeln und zu hosten.

2009

AWS baut in Irland sein erstes Rechenzentrums-Cluster («AWS Region») ausserhalb der USA. **Alibaba Cloud** «erblickt das Licht der Welt».

2010

Dropbox verlässt die Betaphase und wird in der ersten stabilen Version 1.0 veröffentlicht. **Google** lanciert Google Cloud Storage. **Microsofts** Windows Azure Platform ist kommerziell erhältlich.

2013

Oracle schliesst seine Datenbank an die Cloud an. IBM übernimmt den Web-Hoster Softlayer, um eine eigene Cloud-Division zu formen.

2014

Aus Windows Azure wird **Microsoft** Azure. Später im Jahr gibt das Unternehmen Einblick in Azure Machine Learning (ML).

2015

Swisscom lanciert mit der Application-Cloud ein Platform-as-a-Service-Angebot. **Alibaba Cloud** lanciert in China seine KI-betriebene Datenanalyse-Plattform DT PAI. **AWS** kündigt die Plattform Amazon Machine Learning Service an, die Entwickler dabei unterstützen soll, smarte datengetriebene Applikationen zu kreieren. Später im Jahr lanciert AWS ausserdem AWS IoT, seine Managed-Cloud-Plattform für IoT.

2016

IBM startet das Programm «IBM Quantum Experience», in dessen Rahmen Interessierte über die Cloud Zugriff auf einen 5-Qubit-Quantencomputer erhalten. In den kommenden Jahren werden die zur Verfügung gestellten Quantencomputer leistungsfähiger. Interessierte können über die Cloud Algorithmen testen und mit Quantenprozessoren experimentieren.

2017

Swisscom lanciert die Enterprise Service Cloud, eine Schweizer IaaS-Lösung in einer Private Cloud. **AWS** stellt Amazon Sagemaker vor, eine ML-Plattform, auf der Entwickler ML-Modelle kreieren, trainieren und einsetzen können.

2018

Swisscom geht strategische Partnerschaften mit Microsoft und AWS ein. Microsofts Azure IoT Central hilft beim Kreieren und Managen von IoT-Anwendungen. Auch **Google** lanciert eine IoT-Plattform.

Oracle lanciert eine autonome Datenbank, die sich selbst patcht und verwaltet. **Alibaba Cloud** lanciert eine Plattform fürs Kreieren von Blockchain-Anwendungen.

2019

Microsoft startet die Beta für Azure Quantum. Damit sollen User per Azure Cloud Zugriff auf Quantencomputing erhalten. Ausserdem startet das Unternehmen seine Schweizer Cloud. Auch **Google** eröffnet seine Schweizer Cloud-Region. **Oracle** eröffnet sein erstes eigenes Rechenzentrum in der Schweiz.

2020

Aufgrund der Coronapandemie beschleunigen viele Firmen ihre Cloud-Migration – gemäss einer globalen Umfrage von Flexera setzt inzwischen die Mehrheit der Unternehmen auf eine Multi-Cloud-Strategie.

AWS bringt Amazon Braket auf den Markt. Damit erhalten User per Cloud Zugriff auf Quantencomputing und Quantencomputer-Simulatoren.

2022

AWS eröffnet in Zürich seine erste Schweizer Infrastruktur-Region. Und **Swisscom** geht mit seinem AWS-Angebot an den Start. Neu bietet der Telko eine Direktanbindung an die Schweizer Cloud-Region des Hyperscalers an – zusätzlich zur Anbindung an die Azure-Cloud von Microsoft.

Proton lanciert Google-Drive-Alternative

Den vollständigen Artikel finden Sie online
www.netzwoche.ch

ych/yzu. Das Genfer Unternehmen Proton, Anbieter des E-Mail-Verschlüsselungsdienstes Protonmail, hat das Cloud-Speicherangebot Proton Drive lanciert. Die Betaversion dieser Lösung war bereits seit mehreren Jahren verfügbar. Um seine Alternative zu Google Drive und Dropbox zu entwickeln, hatte das in Plan-les-Ouates ansässige Unternehmen 2019 einen Zuschuss von 2 Millionen Euro im Rahmen des europäischen Programms Horizon 2020 erhalten. Proton Drive wurde als durchgehend verschlüsselter Cloud-Speicherdienst vorgestellt und erhielt Feedback von 450 000 Beta-Testern.

«Durch unsere Verwendung von End-to-End-Verschlüsselung sind wir in der Lage, die Vertraulichkeit von Offline-Speicherung und die Bequemlichkeit und Zuverlässigkeit von Cloud-Speicherung zu bieten», schreibt Proton-CEO Andy Yen in einem Blogbeitrag. Für Privatpersonen gibt es eine kostenlose Version inklusive 1 GB Speicherplatz. 500 GB kosten 11.99 Franken pro Monat; bei 12- oder 24-Monatsplänen gibt es Rabatt.

Google schützt vor Cryptomining in der Cloud

rja. Google hat eine neue Schutzfunktion für seine Cloud-Umgebung vorgestellt. Virtual Machine Threat Detection (VMTD) bietet agentenloses Speicherscanning, um Bedrohungen wie Kryptomining-Malware zu erkennen, wie Google mitteilt.

Der Verzicht auf einen Agenten bedeutet laut dem Unternehmen, dass Kundinnen und Kunden keine zusätzliche Software in ihren Instanzen installieren müssen, um die Schutzfunktion zu nutzen. Dies bedeute auch weniger Leistungseinbussen, einen geringeren Aufwand für die Bereitstellung und Verwaltung von Agenten sowie eine geringere Angriffsfläche für potenzielle Angreifer. Stattdessen modifiziert Google bei VMTD den Hypervisor, also die unter den virtuellen Maschinen der Cloud-Nutzerinnen und -Nutzer arbeitende Software.

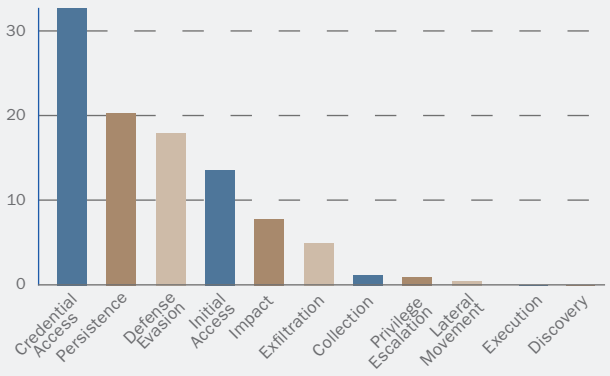
VNTD erkenne Cryptomining zuverlässig, schreibt Google. In den kommenden Monaten soll der Dienst ausgebaut werden und etwa Datenexfiltration und Ransomware erkennen können. Google führt VMTD zunächst als Opt-in-Service für User von Security Command Center Premium ein.

Den vollständigen Artikel finden Sie online
www.netzwoche.ch

Cybergauner greifen Clouds gerne mit echten Accounts an

cka. Elastic hat sich in seinem Global Threat Report unter anderem mit Cloud-Security befasst. Das Unternehmen hinter der Suchmaschine Elasticsearch analysierte dafür die Telemetriedaten der Kunden, die Elastics SIEM-Detection-Rules nutzen.

EINORDNUNG DER ALERTS NACH DEM «ATT&CK»-LEITFADEN



Quelle: Global Threat Report 2222

Das Unternehmen ordnete die registrierten Alerts nach dem «ATT&CK»-Leitfaden von Mitre ein. Die Abkürzung steht für Adversarial Tactics, Techniques and Common Knowledge. Der Leitfaden dient zur Klassifizierung von Taktiken, die bei Cyberangriffen zum Einsatz kommen. Laut der Studie fällt fast ein Drittel der Meldungen in die Kategorie Credential Access – es handelt sich also um Versuche, sich über bestehende Accounts Zugriff zu verschaffen. Dazu nutzen Cyberkriminelle etwa Keylogging, Credential Dumping oder auch Brute-Force-Attacken. Wie Elastic schreibt, bevorzugen es Cyberkriminelle, über bestehende Accounts einzudringen, weil ihre Machenschaften den Admins so weniger schnell auffallen.

Ferner bemühen sich Cyberkriminelle gemäss den Daten von Elastic auch darum, auf den infiltrierten Systemen Persistence zu erreichen. Knapp über 20 Prozent der Alerts ordnete das Unternehmen in diese Kategorie ein. Danach fallen die Prozentwerte rasch ab: rund 17 Prozent für Defensive Evasion, über 13 Prozent für Initial Access, etwa 8 Prozent für Impact (Manipulation und Löschen von Daten) und etwa 5 Prozent für die Exfiltration von Daten.

Den vollständigen Artikel finden Sie online
www.netzwoche.ch

Cloud-Security-Spezialisten sind gefragt wie nie


Gorodenkoff Productions OU / AdobeStock.com

yzu. Fortinet stellt in seinem «Cybersecurity Skills Gap Report» fest: Mangelnde Cybersecurity-Kenntnisse sind verantwortlich für 80 Prozent der Sicherheitsvorfälle. Fortinet befragte mehr als 1200 IT- und Cybersecurity-Entscheider in 28 Märkten. 64 Prozent der Unternehmen erlitten durch Sicherheitsvorfälle einen finanziellen Schaden, 38 Prozent meldeten gar einen Verlust von mehr als einer Million US-Dollar. Doch mangelnde Kenntnisse sind nicht das einzige Problem. Laut einer weiteren Studie von ISC fehlen weltweit mehr als 2 Millionen Cybersecurity-Experten. Dementsprechend gaben 60 Prozent der von Fortinet befragten Führungskräfte an, Probleme bei der Rekrutierung von Cybersecurity-Spezialisten zu haben. 52 Prozent bekunden ausserdem Mühe, qualifiziertes Personal zu halten.

Cloud-Security-Spezialisten gesucht

Den Ergebnissen zufolge ist es am schwierigsten, die Position des «Cloud Security Specialist» zu besetzen. Entsprechende Fachkräfte seien gefragt wie nie. Die Hälfte der Befragten gab an, aktiv auf der Suche nach IT-Security-Talenten mit Spezialisierung auf Cloud-Technologien zu sein. 57 Prozent der befragten Unternehmen bekunden Mühe mit der Einstellung einer solchen Fachkraft. An zweiter Stelle der am häufigsten gesuchten Profile folgen «Security Operations (SOC) Analysts». 42 Prozent der befragten Unternehmen gaben an, nach solchen Fachkräften zu suchen.

Den vollständigen Artikel finden Sie online
www.netzwoche.ch

Datenschutzbeauftragte kritisieren Zürcher Microsoft-365-Entscheid

rja. Im Frühling 2022 hat der Regierungsrat des Kantons Zürich die Nutzung von Microsoft 365 für die Verwaltung bewilligt (mehr dazu lesen Sie auf Seite 42). Die Entscheidung ist allerdings umstritten, wie eine Stellungnahme von Privatim, der Konferenz der Schweizerischen Datenschutzbeauftragten, zeigt. Die Organisation warnt davor, den Beschluss als «Freipass für die Einführung von Microsoft 365 in der Verwaltung» anzusehen.

Auf Kritik stösst die Begründung des regierungsrätlichen Entscheids. Sie wirke «ausgesprochen unausgewogen», schreibt Privatim. So stelle der Regierungsrat etwa fest, dass bei Cloud-Lösungen grundsätzlich keine höheren Risiken für die Informationssicherheit und den Datenschutz bestünden als bei On-Premise-Lösungen. Diese Aussage sei angesichts der diversen zusätzlichen Risiken «nicht nachvollziehbar», kommentiert Privatim. Zu kurz kommt laut der Organisation etwa der Aspekt des Kontrollverlusts. Hier liege es in der Pflicht der öffentlichen Organe, angemessene Massnahmen zu treffen, um den Kontrollverlust zu minimieren.

Den vollständigen Artikel finden Sie online
www.netzwoche.ch

Cloud Act bleibt illegal

Privatim thematisiert auch den möglichen Zugriff US-amerikanischer Strafverfolgungsbehörden auf die in der Cloud gespeicherten Daten, gestützt auf den Cloud Act. In seinem Beschluss hatte der Zürcher Regierungsrat argumentiert, ein solches Szenario sei in der Praxis höchst unwahrscheinlich; zudem habe Microsoft laut eigener Auskunft noch nie Daten europäischer Kunden offenlegen müssen.

Ein solcher Zugriff sei in der Schweiz widerrechtlich und verletze den Datenschutz, hält Privatim dagegen, und zwar unabhängig von seiner statistischen Wahrscheinlichkeit. Die Auskunft von Microsoft sei zudem wenig repräsentativ, «weil die öffentlichen Organe erst jetzt daran sind, die Auslagerung von Daten in die Cloud zu prüfen, sodass Zugriffe auf deren Daten bisher noch gar nicht vorkommen konnten».

«Mega»-Cloud mit Sicherheitslücke

Ein Team von Kryptografinnen und Kryptografen der ETH Zürich hat den Cloud-Dienst des neuseeländischen Anbieters Mega eingehend getestet. Dabei entdeckten sie Sicherheitslücken, die es dem Anbieter ermöglichen, Kundendaten zu entschlüsseln und zu manipulieren. Autor: Markus Gross, ETH Zürich

Den vollständigen Artikel finden Sie online
www.netzwoche.ch

Wie viele Anbieter von Cloud-Lösungen verspricht auch der neuseeländische Provider Mega, dass nicht mal das Unternehmen selbst die Daten der Kunden einsehen oder verändern könne. Dabei geht es nicht nur um die Frage, ob die Kunden dem Anbieter vertrauen, sondern auch darum, dass grosse IT-Dienstleister mit Millionen von Kunden und Milliarden an gespeicherten Dateien, wie Mega, zwangsläufig ins Visier von Geheimdiensten, Regierungen oder Personen mit kriminellen Absichten geraten. «Man kann bei keinem grossen Cloud-Anbieter ausschliessen, dass seine Systeme kompromittiert sind», sagt Kenneth Paterson. «Ausserdem kommt es auch immer wieder vor, dass Anbieter mit Regierungsorganisationen zusammenarbeiten.» Umso wichtiger ist es, dass einzig die Kunden ihre Cloud-Daten entschlüsseln können.

Die ETH-Kryptografieexperten Matilda Backendal, Miro Haller und Kenneth Paterson haben die Verschlüsselung von Mega getestet und sind dabei auf gravierende Sicherheitslücken gestossen. Diese ermöglichen es dem Anbieter – oder Dritten, die sich Zugriff auf die Server von Mega verschaffen –, Kundendaten zu entschlüsseln, zu verändern oder gezielt Daten auf dem Speicher der Kunden zu platzieren.

Kenneth Paterson, Professor für Informatik an der ETH Zürich.
Bild: inf.ethz.ch

Grundlegende Schwachstelle: ein Schlüssel für alles

Paterson und sein Team analysierten den Quellcode der Software und stiessen dabei auf mehrere kritische Sicherheitslücken. Um die Effektivität der Angriffe zu testen, bauten sie die Plattform der Neuseeländer teilweise nach und versuchten, die persönlichen Konten der Forschenden anzugreifen.

Wenn ein User auf sein Mega-Konto zugreift, kann durch eine Manipulation der Sitzungs-ID der private RSA-Schlüssel des Users innerhalb von maximal 512 Login-Vorgängen gestohlen werden. Dieser Schlüssel wird zum Austauschen von Daten benutzt. Durch eine zusätzliche Manipulation der Mega-Software auf dem Computer des Opfers kann man das betroffene Benutzerkonto dazu bringen, sich automatisch immer wieder einzuloggen. Dies verkürzt die Dauer bis zur vollständigen Offenlegung des Schlüssels auf wenige Minuten. Da die Schlüssel für die Dateiverschlüsselung auf dieselbe Weise geschützt werden, können Angreifer aufbauend auf dem Wissen aus der ersten Attacke auch alle weiteren Schlüssel offenlegen.

Daten stehlen, manipulieren oder selbst hochladen

Nun haben die Angreifer kompletten Zugriff auf die unverschlüsselten User-Daten und können diese kopieren und manipulieren. Eine zusätzliche Angriffsvariante ermöglicht es sogar, beliebige Daten in das Cloud-Laufwerk des Opfers hochzuladen. So können die Täter das Opfer betrügen oder erpressen, indem kontroverses, illegales oder kompromittierendes Material in dessen Dateispeicher eingefügt wird. Das Opfer wiederum hat keine Chance, nachzuweisen, dass es das Material nicht selbst hochgeladen hat.

Die Forschenden der ETH haben die gefundenen Schwachstellen gegenüber Mega offengelegt. «Zusätzlich haben wir Mega einen dreistufigen Massnahmenplan vorgelegt, der aufzeigt, wie die Sicherheitslücken behoben werden könnten», so Paterson. In einer ersten Phase empfahl das Team eine Reihe von Sofortmassnahmen, welche die Benutzer vor den schwerwiegendsten Sicherheitsproblemen schützen. Die zweite Phase sieht umfangreichere Änderungen vor, um Angriffe effizienter abzuwehren, ohne dass kostspielige Änderungen wie die Neuverschlüsselung von Daten vorgenommen werden müssen. Die dritte Phase umfasst langfristige Ziele für die Neugestaltung der kryptografischen Architektur. «Das Unternehmen hat jedoch andere Massnahmen ergriffen als diejenigen, die wir vorschlugen», sagt Paterson. Sie vermögen aber den ersten Angriff – also denjenigen auf den RSA-Key – zu verhindern.

Dieser Beitrag ist zuerst bei ETH News erschienen.

IT-Sicherheit: Den Datenschatz im Unternehmen identifizieren und schützen

Cybersicherheit in Unternehmen ist komplex. Für den bestmöglichen Schutz ist es essenziell, zu wissen, welche Daten und Systeme besonders schützenswert sind, um dann gezielt eine Sicherheitsstrategie aufzubauen.

Den Beitrag finden Sie auch online
www.netzwoche.ch

Die Autorin
Cornelia Lehle, Head of Sales DACH, G Data Cyberdefense

Unternehmensdaten sind ein beliebtes Ziel von Cyberkriminellen. Wenn es Angreifern gelingt, solche Informationen zu erbeuten oder mit Ransomware zu verschlüsseln, wird es teuer für die Opfer. Aber nicht alle Daten haben den gleichen Wert. Wer die wichtigsten Vermögenswerte im Unternehmen identifiziert, kann Cyberbedrohungen gezielt angehen. Die Ermittlung dieser Kronjuwelen ist hilfreich, um eine gute IT-Sicherheitsstrategie und einen Plan für die Reaktion auf Zwischenfälle festzulegen. Wer keine Ahnung hat, was schützenswert ist, kann auch nicht wissen, wie effektiver Schutz aussieht. Grundsätzlich gilt: Alle Daten können kritisch sein, seien es Mitarbeiter- oder Kundendaten, Geschäftsgeheimnisse oder andere Daten.

Zugangsdaten in falschen Händen

Ein grosses Risiko für Unternehmen sind ausgeleitete Zugangsdaten in den falschen Händen. Bei mehr als 60 Prozent der IT-Sicherheitsvorfälle in den vergangenen Jahren wurden Zugangsdaten missbraucht. Und jedes Jahr tauchen Millionen dieser Daten im Dark Web auf. Cyberkriminelle erwerben diese Informationen, um in Unternehmensnetzwerken Fuss zu fassen, Daten zu exfiltrieren und vieles mehr. Aber genau hier liegt das Problem: Wenn Zugangsinformationen gestohlen werden, fällt dies kaum auf. Die Ausnahme: Eine unberechtigte Person macht auffällige Dinge. Andernfalls bleibt der Verlust unbemerkt. Denn das «gestohlene» Passwort kann der ursprüngliche Besitzer weiterhin nutzen. Daher ist es entscheidend, Login-Daten, die in falsche Hände geraten sind, frühzeitig etwa auf einer Dark-Web-Marktplattform zu finden.

Kronjuwelen schützen – aber?

Um Unternehmen vor Cybergefahren zu schützen, ist eine aktuelle Endpoint-Protection-Lösung unabdingbar. Sie entlarven und wehren Backdoors, RATs (Remote Access Trojans) und Spyware ab. Da aber auch Social-Engineering-Angriffe Datenverluste verursachen, sollten Unternehmen zusätzlich das Sicherheitsbewusstsein ihrer Mitarbeitenden durch Awareness-Schulungen stärken.

Ein weiterer Schutzfaktor ist die Multifaktor-Authentifizierung (MFA), die den Anmeldeprozess um eine ergänzende Schutzebene erweitert. Beim Zugriff auf Konten führen Nutzerinnen und Nutzer eine zweite Identitätsprüfung durch, indem sie beispielsweise einen Fingerabdruck scannen. Dieser zweite Faktor macht die erbeuteten Zugangsdaten wertlos.

Ein «fortschrittliches» IT-Sicherheitsteam in einem grossen Unternehmen kann aber noch mehr tun:

- Das Dark Web überwachen und versuchen, geschlossene Quellen zu infiltrieren, was leichter gesagt, als getan ist.
- Automatisiert Tor-Seiten, Foren, Shops und Märkte analysieren.
- Zugang zu verschiedenen Quellen für geleakte Zugangsdaten verschaffen, wie Dark Web, Paste Sites und Data Dumps.

Zugegeben: Diese Überwachung ist für KMUs schwierig. Wer aber über einen guten Sicherheits- und Reaktionsplan verfügt, ist besser auf einen Cyberangriff vorbereitet.

Configuration Management: Die Basis für den sicheren Modern Workplace

In der modernen Arbeitswelt werden Endgeräte zunehmend verwundbarer. Es gilt deshalb, Systeme, Applikationen, User, Policies sowie Privilegien vollumfänglich zu konfigurieren und zu überwachen. Eine entscheidende Rolle spielt dabei das Configuration Management.

Autor: Kurt Ris, CEO und Mitgründer, Everyware

Ein Modern Workplace bietet Unternehmen jene Flexibilität, welche die heutige Arbeitswelt von ihnen verlangt. Gesucht sind Wege, die neue Art des Arbeitens sinnvoll mit den individuellen Möglichkeiten und Bedürfnissen zu kombinieren. Diese Flexibilität bringt jedoch auch grosse Herausforderungen mit sich. Der Modern Workplace muss nicht nur die Zusammenarbeit mittels Videokonferenzen ermöglichen, sondern unter anderem auch – und das ist fast noch wichtiger – den Zugriff auf firmeninterne Daten sicherstellen oder das Ausführen von geschäftskritischen Anwendungen erlauben. Gefragt ist deshalb eine clevere Modern-Workplace-Strategie, die den Anforderungen der neuen Arbeitswelt gerecht wird.

Auf die richtige Konfiguration kommt es an

Zwingende Bestandteile dieser Strategie müssen IT-Sicherheit, Datenschutz und Compliance sein. Denn beim Shift in die Cloud und beim mobilen Arbeiten bleibt das Endgerät nach wie vor ein wichtiger Dreh- und Angelpunkt – und insbesondere das wird zunehmend verwundbarer. Mitarbeitende greifen nicht mehr nur aus dem Firmennetz auf vertrauliche und personenbezogene Daten zu, sondern nutzen Collaboration- und Speicherlösungen auch aus dem Home- oder Mobile-Office. Dies bedingt ein Umdenken hinsichtlich des Security-Ansatzes und verlangt Massnahmen wie beispielsweise eine Strong Authentication oder eine Segmentierung der Daten. In Compliance-sensiblen Branchen führt daran kein Weg vorbei. Aber auch Unternehmen aus anderen Branchen sollten sich stärker damit befassen.

Bild: ST.art / AdobeStock.com

Wichtig hierbei ist das Configuration Management. Dabei geht es um die vollumfängliche Verwaltung der Endgeräte. Mithilfe von Automatisierungstools wie Microsoft Intune werden Systeme, Applikationen, User, Policies sowie Privilegien konfiguriert und gleichzeitig überwacht. Als sogenannte Cloud Governance wird dabei das Regelwerk bezeichnet, das dem Configuration Management zugrunde liegt. Dieses umfasst eine Reihe von Praktiken, die dazu beitragen, dass Nutzerinnen und Nutzer in der Cloud so arbeiten, wie es die Unternehmensrichtlinien vorsehen, dass der Betrieb effizient ist und er überwacht sowie bei Bedarf korrigiert werden kann. Ein solches Cloud Governance Framework soll so gestaltet sein, dass es Teams unterstützt, statt einschränkt oder zurückbindet. In der Praxis wird damit zum Beispiel verhindert, dass einzelne User innerhalb einer Organisation in Microsoft Teams zu viele Berechtigungen erhalten und so zum Sicherheitsrisiko werden. Folglich zielt ein Cloud Governance Framework mitunter darauf ab, Gruppierungen, Freigabeberechtigungen, Datensensibilität, Lebenszyklen und andere Komponenten zu definieren.

Gemanagt, bedarfsgerecht konfiguriert und massgeschneidert

Für Unternehmen empfiehlt es sich deshalb, auf einen versierten Partner mit Erfahrung zu setzen, der nicht nur Endpoints unternehmensweit managt und gleichzeitig Rollen, Policies sowie Privilegien bedarfsgerecht konfiguriert, sondern das darunterliegende Framework gleich auch gemeinsam mit den Kunden individuell erarbeiten kann. Dies ermöglicht es, dass auch Unternehmen wie Banken und Versicherungen ihre IT-Landschaft entsprechend gestalten sowie gemäss den Governance- und Compliance-Richtlinien arbeiten können. Schliesslich kommt die IT – egal ob bei grösseren oder kleineren Unternehmen – heute ohne solides Configuration Management, das auf einer sinnvollen Basis aufbaut, nicht mehr aus.

Das Dosier finden Sie auch online
www.netzwoche.ch

«IT-Security muss im Kontext des Public-Cloud-Einsatzes neu gedacht werden»

Unternehmen, die eine Public Cloud nutzen, müssen ihre IT-Security entsprechend anpassen. Welche Schritte notwendig sind und was Firmen berücksichtigen sollten, erklärt Kurt Ris, CEO und Mitgründer von Everyware. Interview: Tanja Mettauer

Kurt Ris, CEO und Mitgründer, Everyware.

Welches sind die wichtigsten Aspekte, die das Cloud-Governance-Framework umfasst?
Kurt Ris: Ein solches Framework kann sehr vielschichtig sein. Das Wichtigste ist jedoch, dass es praktikabel zum jeweiligen Unternehmensziel beziehungsweise zur Business-Strategie passt. Es ist wichtig, dass das Unternehmen sich damit auseinandersetzt, wie es mit der Nutzung der Cloud im Unternehmen umgehen will. Heisst: Will man ein starres Regelwerk schaffen oder den Mitarbeitenden möglichst viel Freiheit bieten? Ein weiterer wichtiger Aspekt der Governance sind hier etwa Compliance und Security. Die IT-Security muss im Kontext des Public-Cloud-Einsatzes neu umfassend gedacht und festgehalten werden.

Wie kann ein automatisiertes Configuration Management helfen, diesen Wildwuchs bei der Endgeräteverwaltung zu bekämpfen?
Das Configuration Management unterstützt Administratorinnen und Administratoren bei der Verwaltung von Endgeräten und erlaubt es ihnen, Einstellungen äusserst granular festzulegen sowie anschliessend über ein ganzes Unternehmen hinweg auszurollen und zu orchestrieren. Wird nun zum Beispiel bei einem firmenweiten Deployment das einheitliche Image einer Anwendung eingesetzt, hilft das dabei, Versionen-Wildwuchs zu verhindern. Ausserdem zwingt das Configuration Management Unternehmen zu einem gewissen Mass an Standardisierung. So trägt dieses automatisch zu einer Reduktion des Wildwuchses bei.

Welche Implementierungsschritte umfasst ein erfolgreiches Configuration Management?
Ein solches Projekt startet bei uns stets mit der Analyse der Ausgangslage, die anschliessend gemeinsam mit dem Kunden besprochen wird. Von Vorteil ist, wenn im Unternehmen bereits ein grundlegendes Framework existiert, das für das Configuration Management eingesetzt werden kann. Danach werden Bedürfnisse sowie die angepeilten Ziele ermittelt und dementsprechend Empfehlungen abgegeben. Erfolgt der Start gewissermassen «auf der grünen Wiese», dann beginnt man zunächst damit, grundlegende Parameter zu definieren, die dann in konkrete Massnahmen wie Policies, Gruppeneinteilungen oder Berechtigungen umgemünzt werden können.

Für welche Unternehmen eignen sich Automatisierungstools wie Microsoft Intune?
Automatisierungstools werden in der Handhabung immer mächtiger und granularer. Deshalb braucht es Spezialisten-Know-how. Trotzdem eignen sie sich grundsätzlich sowohl für KMUs als auch für Grossunternehmen; ein Microsoft Endpoint Manager insbesondere für diejenigen, die den Microsoft Office 365 Stack im Einsatz haben. Voraussetzung ist jedoch eine gewisse Anzahl an User und Devices, damit der Einsatz überhaupt Sinn ergibt. Ergänzend kommt selbstverständlich auch ein Mindestmass an Digitalisierung der Prozesse und Abläufe hinzu.

Welche Aufgaben und Prozesse können Automatisierungstools für die Firmen konkret übernehmen?
Klassischerweise kommen sie in wiederkehrenden, repetitiven Prozessen zum Einsatz. Im Zusammenhang mit dem Configuration Management hilft die Automatisierung insbesondere dabei, dass auch grosse Systeme überwacht werden können. Gerade aus Sicht der IT-Security sind hier bewusst gesetzte Kontrollinstanzen besonders wichtig. Damit lässt sich einerseits prüfen, ob die installierten Sicherheitsvorkehrungen auch wirklich greifen, und ob sie andererseits keine Einschränkung für die Mitarbeitenden darstellen.

Bild: macrovectror / Freepik.com

Was es für einen sicheren Shift in die Cloud braucht

yzu. Cloud liegt im Trend, sei es eine Private oder Public Cloud, ob man eine Hybrid-, Single- oder Multi-Cloud-Strategie verfolgt. Unternehmen bietet die Cloud durchgehende Verfügbarkeit und ermöglicht Zugriff auf Firmendaten von überall auf der Welt. Doch diese Erreichbarkeit macht die Cloud auch anfällig für Cyberangriffe.

Ein Wechsel in die Cloud erfordert daher einige Überlegungen, von der Wahl des Providers über das Bestimmen der zu migrierenden Systeme bis zum Festlegen von Sicherheitskonzepten. Doch wie genau bereiten Unternehmen diesen Wechsel am besten vor? Welche neuen Sicherheitsrisiken entstehen beim Wechsel in die Cloud? Und welche Herausforderungen stellen sich beim Aufbau einer wirklich sicheren Cloud-Infrastruktur? Darüber diskutieren Experten von Baggenstos, Die Mobiliar, Elca, Equinix, Google Cloud Schweiz und Redhat im Podium.

« EIN MINIMALES RISIKO BESTEHT ALLENFALLS IN EINER GEWISSEN ABHÄNGIGKEIT VON EINEM ANBIETER »

Michael Kistler
CEO, A. Baggenstos & Co.

Welche Vorbereitungen müssen Unternehmen treffen, bevor sie in die Cloud gehen?
Michael Kistler: Es empfiehlt sich, schon früh einen kompetenten Cloud-Partner einzubeziehen, der über fundierte Erfahrung in der Cloud-Migration verfügt. Zusammen mit diesem Partner beginnt man mit einer fundierten Analyse der Ist-Situation und der Anforderungen an die neue Cloud-Lösung. Je nach Branche sind die spezifischen Compliance-Anforderungen relevant. Wichtig ist zudem, die Fachbereiche miteinzubeziehen, um die relevanten Eckpunkte für das Business zu definieren.

Welche Sicherheitsrisiken ergeben sich mit einem Wechsel in die Cloud?
Wir sehen in der Regel eine Reduktion der Risiken, wenn man in die Cloud wechselt. Wir haben viel mehr Möglichkeiten und Werkzeuge, die Sicherheit von Daten und Anwendungen in der Cloud zu gewährleisten. Ein minimales Risiko besteht allenfalls in einer gewissen Abhängigkeit von einem Anbieter. Die führenden Provider sind aber heute maximal abgesichert, und grössere Ausfälle waren in den letzten Jahren kaum zu verzeichnen.

Was sind die grössten Herausforderungen beim Aufbau einer sicheren Cloud-Umgebung?
Es gilt, von Anfang an die Enterprise-Security-Architektur der Cloud-Infrastrukturen zu nutzen. Oft empfiehlt es sich auch, Legacy-Applikationen im Vorfeld in einem Proof of Concept zu testen, um sicherzustellen, dass Sicherheit und Funktionalität auch in der Cloud gewährleistet werden können.

« UNTERNEHMEN ERHÖHEN DURCH DIE VERLAGERUNG IN DIE CLOUD IHR GESAMTRISIKO »

Fabrice Guye
Senior Business Development and Sales Manager, Senthorus, an Elca Security Company

Welche Vorbereitungen müssen Unternehmen treffen, bevor sie in die Cloud gehen?
Fabrice Guye: Sie müssen sich mehrere Fragen stellen. Die ersten sind einfach: Gibt es einen Grund für die Verlagerung in die Cloud, und wird durch eine solche Verlagerung ein geschäftlicher Nutzen geschaffen? Wenn die Antwort «Ja» lautet, und das ist in den meisten Fällen so, dann stellt sich die Frage nach den Risiken. Welchen neuen Risiken ist das Unternehmen durch die Cloud ausgesetzt, und was sind die Kronjuwelen, die in die Cloud verschoben werden? Sobald diese Fragen beantwortet sind, kann eine geeignete Cloud-Strategie für eine erfolgreiche Implementierung entwickelt werden. Die Hauptziele sind immer, den Bedarf und den Zweck zu klären und dann den Übergang zu gestalten.

Welche Sicherheitsrisiken ergeben sich mit einem Wechsel in die Cloud?
Es gibt viele, aber das wichtigste Risiko liegt auf der Hand: Der Wechsel in die Cloud bedeutet, dass man sich in einer Art offenen Umgebung bewegt, die über das Internet zugänglich ist. Es gibt wenig Spielraum für Konfigurationsfehler, da andere (einschliesslich Hacker) live nach Problemen suchen. Eine Fehlkonfiguration könnte oder würde direkt zu einem Datenleck führen, was nicht der Fall ist, wenn Unternehmen ihre Server selbst hosten. Man könnte auch argumentieren, dass Unternehmen durch die Verlagerung in die Cloud ihr Gesamtrisiko erhöhen (was richtig ist) und neue Risiken schaffen, zum Beispiel rechtmässiges Abfangen wie beim US-amerikanischen Cloud Act.

Was sind die grössten Herausforderungen beim Aufbau einer sicheren Cloud-Umgebung?
Es ist immer schwierig, über die grössten Herausforderungen zu sprechen, da sie stark vom jeweiligen Kontext abhängen. Für einige Branchen wie das Finanzwesen ist beispielsweise eine angemessene Ausstiegsstrategie unerlässlich. Im Gegensatz dazu haben einige andere Branchen mehr Bedenken hinsichtlich der Datenresidenz; für andere ist es die Kontinuität des Betriebs. Generell würde ich jedoch das Thema Vendor Lock-in als kritisch und herausfordernd bezeichnen, insbesondere für alles, was mit SaaS-Anwendungen zu tun hat. Wenn ich aber ein Thema spezifizieren müsste, dann wäre es, dass es nicht mehr nur eine einzige Cloud gibt, da die meisten Unternehmen auf eine Mischung aus öffentlichen, privaten und hybriden Umgebungen (IaaS und Saas) setzen. Das bringt natürlich Komplexität in Bezug auf Identitäts- und Zugriffsmanagement (IAM) sowie Compliance mit sich, aber die Kenntnis mehrerer Umgebungen bedeutet auch zusätzliches, umfangreiches Fachwissen.

« DAS VERTRAUEN IN DIE SICHERHEITSANBIETER MUSS SEHR HOCH SEIN »

Juergen Kaus
Senior Solutions Architect Schweiz und Irland, Equinix

Welche Vorbereitungen müssen Unternehmen treffen, bevor Sie in die Cloud gehen?
Juergen Kaus: Auf die Frage: Warum gehen wir in die Cloud?, sollte die Antwort nicht lauten: Weil viele es tun. Er braucht Antworten auf die Fragen: Was, in welcher Reihenfolge wird in die Cloud übertragen? Kann ich heute schon mehr als einen Cloud-Provider ausmachen? In welcher Zeit kann ich mein Unternehmen für die Cloud vorbereiten? Welche Schulungen und neuen Personen benötige ich? Kann ich Erfahrungen wiederverwenden?

Welche Sicherheitsrisiken ergeben sich mit einem Wechsel in die Cloud?
Dienstleister haben Zugriff auf essenzielle Sicherheitssysteme; Kunden aber haben nur begrenzt Einsicht in diese Teams, das heisst, das Vertrauen in die Sicherheitsanbieter muss sehr hoch sein. Schnelle Wechsel zu einem neuen Sicherheitsanbieter sind mit hohen Investitionen und langen Prozessen verbunden.

Was sind die grössten Herausforderungen beim Aufbau einer sicheren Cloud-Umgebung?
Den verschiedenen Anforderungen der eigenen Abteilungen sowie Partnern Rechnung zu tragen und zur gleichen Zeit die Zukunft im Auge zu behalten: Wohin werde ich mich in ein bis fünf Jahren bewegen?

« HERAUSFORDERND IST DIE SICHERE KONFIGURATION UND ÜBERWACHUNG DER EINGESETZTEN CLOUD-SERVICES UND SCHNITTSTELLEN »

Christian Zeller
CISO, Die Mobiliar

Welche Vorbereitungen müssen Unternehmen treffen, bevor sie in die Cloud gehen?
Christian Zeller: Man muss die Anforderungen aus Sicht des Business erheben und den angestrebten Mehrwert validieren sowie die damit verbundenen Abhängigkeiten und Risiken aus Sicht des Unternehmens. Rechtliche und regulatorische Anforderungen müssen verifiziert und in der spezifischen Umsetzung geklärt und adressiert werden. Zudem muss man den strategischen Ansatz für die Cloud Transition und die Zielarchitektur definieren (Cloud Native oder Lift-&-Shift-Approach), und zwar auf Basis einer ganzheitlichen Planung. Ebenfalls nötig ist es, die veränderte Risikosituation aus der Nutzung der Cloud zu analysieren und zu bewerten (hybride Umgebung On-Prem & Cloud). Die IT-Sicherheitsstrategie und das Target Operating Model (Cloud-Bereitstellungs- und Servicemodell) müssen auf das Cloud-Umfeld adaptiert werden, ebenso die relevanten Sicherheitsprozesse. Ausbildungsinitiativen im Kontext Cloud-Sicherheit und -Nutzung sind zu konzipieren und zu starten. Für die angestrebte Cloud Transition (Cloud Journey) und das zu etablierende Sicherheitsdispositiv ist eine längerfristige Planung zu erstellen.

Welche Sicherheitsrisiken ergeben sich mit einem Wechsel in die Cloud?
Folgende Risiken gilt es abzuwägen:
- die Nutzung von Services mit Datenspeicherung, die nicht den Datenschutzanforderungen entsprechen (z.B. EDÖB-Staatenliste)
- ein möglicher Kontrollverlust und Abhängigkeiten hinsichtlich der Daten und IT-Infrastrukturen (Single Point of Failure)
- mangelnde Datensicherheit in der Datenübertragung beim Zugriff auf diese Daten sowie ungenügender Schutz vor versehentlicher Löschung oder Veränderung von Daten
- regulatorische und rechtliche Risiken, die sich nicht über die Standardangebote und -verträge der Cloud-Anbieter absichern lassen (unter anderem fehlende Audit- und Weisungsrechte)
- Provider-Abhängigkeiten und Vendor Lock-in
- ein möglicher Verlust des Know-hows beim internen Fachpersonal und fehlende Bestellerkompetenz.

Was sind die grössten Herausforderungen beim Aufbau einer sicheren Cloud-Umgebung?
Herausfordernd ist die sichere Konfiguration und Überwachung der eingesetzten Cloud-Services und Schnittstellen. Nicht zu unterschätzen ist auch die Komplexität der eingesetzten Cloud-Sicherheitstechnologien und der notwendigen Transparenz zur laufenden Steuerung und Kontrolle. Weitere Challenges sind die Integration und Abhängigkeiten zum bestehenden Sicherheitsportfolio (On-Prem) sowie die laufende Adaptierung und Ausrichtung des Sicherheitsportfolios aufgrund des sich rasch verändernden Umfelds bei den Anbietern (Kadenz der Weiterentwicklung). Schwierigkeiten bereitet allenfalls auch das fehlende Know-how der Fachspezialisten für die Definition der notwendigen Sicherheitspolicies und deren Kontrolle hinsichtlich der verwendeten Cloud-Technologien und -Services.

« SCHLECHT GEPLANTE IT-ARCHITEKTUR IST AUCH IN DER CLOUD NICHT LEISTUNGSFÄHIG »

Christian Federkiel
Customer Engineering Manager,
Google Cloud

Welche Vorbereitungen müssen Unternehmen treffen, bevor sie in die Cloud gehen?
Christian Federkiel: Unerlässlich ist, dass unsere Kunden klare Ziele haben und sich den genauen Anwendungszweck ihrer Cloud-Anwendungen bewusst machen. Aufgrund dieser Analyse können wir in die gemeinsame Planungsphase gehen. Schlecht geplante IT-Architektur ist auch in der Cloud nicht leistungsfähig. Entscheidend ist weiter, dass die Mitarbeitenden richtig geschult werden. Wir unterstützen deshalb tatkräftig mit unserer Erfahrung, mit Beispielen und Referenzarchitekturen.

Welche Sicherheitsrisiken ergeben sich mit einem Wechsel in die Cloud?
Unternehmen jeglicher Art und Grösse stehen heute einer Vielzahl von Cyberbedrohungen gegenüber: Hacking, Phishing, Ransomware, Malware-Angriffe etc. Besonders bei Unternehmen mit weniger verfügbaren IT-Sicherheitsressourcen haben es Cyberkriminelle oft leichter, Schwachstellen zu finden – unabhängig davon, wo sich die Daten befinden. Wir empfehlen daher immer eine tiefgründige Planung in Bezug auf IT-Sicherheit.

Was sind die grössten Herausforderungen beim Aufbau einer sicheren Cloud-Umgebung?
Hohe IT-Sicherheitsstandards zu entwickeln und umzusetzen, ist immer eine grosse Herausforderung für Unternehmen. Neben modernen Sicherheitstechnologien und -werkzeugen sollte unbedingt auch ein Augenmerk auf das schwächste Glied der IT-Sicherheitskette – den Menschen – gelegt werden. Oft sind es schwache Passwörter, Fehlkonfigurationen, veraltete Softwarestände, Social Engineering beziehungsweise Malware- und Ransomware-Angriffe, die Cyberkriminellen helfen, relativ einfach Zugang zu Daten oder Rechnerinfrastrukturen zu erhalten. Ausser den bereits genannten Möglichkeiten kann beispielsweise mit der Migration in die Cloud auf ein sogenanntes Zero-Trust-Sicherheitsmodell umgestellt werden, was langfristig mehr Sicherheit bietet.

« AUCH IN DER CLOUD GILT: WER ZULETZT PATCHT, HAT DIE SCHLECHTESTEN KARTEN »

Thomas Bryner
Associate Manager Solution
Architecture, Red Hat Switzerland

Welche Vorbereitungen müssen Unternehmen treffen, bevor sie in die Cloud gehen?
Thomas Bryner: Der Schritt in die Cloud ist grundsätzlich gleich zu behandeln wie der Aufbau eines eigenen Rechenzentrums. Es braucht Gedanken zu Planung, Governance, Security, Services und Prozessen. Hinzu kommen Architektur- und Betriebsüberlegungen. Wichtig ist ausserdem eine klare (betriebswirtschaftliche) Zielsetzung auf Unternehmensebene. Oder noch besser: eine Unternehmensstrategie, welche die Cloud als festen Kern der Wertschöpfungskette versteht.

Welche Sicherheitsrisiken ergeben sich mit einem Wechsel in die Cloud?
Da Unternehmen die Bereitstellung respektive den Betrieb einiger Schichten des IT-Stacks dauerhaft und kaum im Detail beeinflussbar fremd beziehen, müssen vor allem die Übergänge auf Kundenseite sauber geklärt sein. Und grundsätzlich gilt auch in Sachen Cloud: Wer zuletzt patcht, hat die schlechtesten Karten.

Was sind die grössten Herausforderungen beim Aufbau einer sicheren Cloud-Umgebung?
Wenn etwas schnell gehen soll oder mangelnde Automatisierung vorherrscht, dann ist der Human Error meist nicht fern. Der schieren Menge an Patches, CVEs und anderen Anforderungen kann nur mit Automation zielführend begegnet werden. Bei DevOps-Projekten ist dagegen ein konsequenter DevSecOps-Ansatz Pflicht.

Der Geruch des Geldes

tme. Die menschliche Nase ist ein empfindliches und komplexes Organ. Das Riechepithel im Naseninneren nimmt Duftmoleküle aus der Luft auf, die über Riechnerven zum Riechkolben gelangen, bis sie dann im Gehirn ankommen. Auf einige mag dann die Duftexplosion einer Gruppe gut parfümierter Personen anziehend wirken, auf andere abschreckend. Bestimmte Gerüche lassen jedoch fast alle Menschen aufschrecken – wie etwa der Duft nach verbrannten Haaren. Wer nach einem auffälligen Parfüm sucht, hat vielleicht in Elon Musks neuestem kreativen Erguss die gesuchte Duftnote gefunden. Musk lancierte im Oktober ein Parfüm mit dem Namen «Burnt Hair» – zum stolzen Preis von 100 US-Dollar, wie «Der Standard» berichtet. In gewohnter Manier verbreitete Musk die frohe Kunde zum «edelsten Duft der Welt» am 12. Oktober auf Twitter. Und der Unternehmer hat bewiesen, dass er auch mit schlechten Düften Geld machen kann. Die «Essenz des widerwärtigen Verlangens» ist bereits ausverkauft. Musk verkündete am 19. Oktober, dass die limitierte Auflage vergeben sei. Die Flaschen mit der betörenden Duftnote «verbranntes Haar» sollen im ersten Quartal 2023 ausgeliefert werden. Bis dann können wir uns noch auf unsere Nase verlassen und alarmiert umherschauen, wenn wir verbranntes Haar riechen.

Lügen haben kurze Beine – ausser im Metaversum

rja. Noch steht im Metaversum niemand auf eigenen Beinen. Die Avatare, die sich in Mark Zuckerbergs Traumwelt der Zukunft tummeln, haben nämlich schlicht keine und müssen sich als Torsos fortbewegen, wie «Futurezone» schreibt. Dies stört sowohl User als auch die Macherinnen und Macher des Metaversums. Die Freude war darum gross, als Zuckerberg ankündigte, dies ändern zu wollen, und dies mit einem Preview-Video untermauerte. Darauf waren zwar tatsächlich Avatare zu sehen, die hüpfen oder kickboxen konnten. Blöd nur: Das Video zeigte keine Avatare im Metaversum, sondern «Animationen auf Grundlage von Bewegungstrackern», wie «Futurezone» unter Berufung auf «kotaku» schreibt. Im besten Fall sind die Beine der Avatare also einfach noch nicht reif für die Vorführung – im schlechtesten Fall gibt es sie noch gar nicht. Die Moral der Geschichte? Lügen haben kurze Beine. Ausser im Metaversum – da haben sie gar keine.

Merkwürdiges aus dem Web

CE- und IT-Welt fördern immer wieder Erstaunliches und Kurioses zutage, das zum Schmunzeln anregt. Die seltsamsten Kurznews immer in der Rubrik «Curiosities».

Gute Unterhaltung!

Gestohlenes Stöckchen zum Ersten …

jor. NFTs sind wie Globuli: Einige glauben daran, wenige machen damit viel Geld – und niemand weiss, wozu sie gut sind. Im Gegensatz zur Homöopathie haben die digitalen Echtheitszertifikate immerhin Unterhaltungswert. So wie die Versteigerung eines NFTs von einem Hundestöckchen zum Startgebot von 1200 US-Dollar. Zum digitalen Bild inklusive Zertifikat gibt's auch das analoge Original: ein 14,5 Zentimeter langer Eichenstock, der «Jahrzehnte lang den Charme, Schmutz und Gestank von New York» aufgesaugt haben soll, wie «T3N» berichtet. Die Versteigerer sind zwei Eheleute, die allerdings verschweigen, dass sie den Kurator – einen dreijährigen Rüden namens Remy – enteignet haben.

Mit Dickpics gegen Ransomware

yzu. Wer Opfer eines Ransomware-Angriffs wird, sollte das Lösegeld nicht bezahlen. Da sind sich Cybersecurity-Expertinnen und -Experten einig. Noch offen ist die Meinung der Experten-Community zur Verteidigungsstrategie der Sambischen Zentralbank. Diese wurde Opfer einer Ransomware-Attacke und erhielt eine Lösegeldforderung von den Cyberkriminellen. Darauf reagierte die «Bank of Zambia» mit einem Link zu einem Dickpic und einer Gebrauchsanweisung, was man mit dem abgebildeten Objekt zu machen habe. Wie der IT-Leiter der Bank gegenüber «Bloomberg» erklärte, wurden gar keine kritischen Daten gestohlen und man hätte gar nicht auf die Erpresser eingehen müssen. Die IT-Verantwortlichen der Zentralbank wollten sich also vor allem einen Spass aus der misslichen Lage machen. Ganz nach dem Motto: ein geschmackloser Streich, wem Geschmackloses gebührt.

Bilder: macrovector/freepik.com; freepik/freepik.com; TeinStud/freepik.com; Antonov Maxim/shutterstock.com; Onion/iStock.com; brgfx/freepik.com; gstudioimagen/freepik.com

CYBERSECURITY

IT-Sicherheit am End-Point und in der Cloud

netzmedien

netzwoche | IT-MARKT | ICTjournal

Markus Stotz
Head of Sales
+41 44 355 63 34 | +41 79 316 60 60
markus.stotz@netzmedien.ch

Colette Mader
Senior Sales Consultant
+41 44 355 63 39 | +41 79 850 10 00
colette.mader@netzmedien.ch

Konstantinos Georgiou
Sales Consultant
+41 44 355 63 33 / +41 79 935 27 93
konstantinos.georgiou@netzmedien.ch

Supannika Chavanne
Senior Sales Consultant
+41 79 255 89 98
supannika.chavanne@netzmedien.ch

MEDIADATEN CYBERSECURITY 2023:

Jetzt Offerte für eine (Print-/Online-)Präsenz in der gewünschten Sprachregion anfordern:

→ **Erscheinungstermine (Print/online):**
08. März 2023 (Deutsch und Französisch) mit Netzwoche und ICTjournal
22. März 2023 mit IT-Markt

→ **Auflage national 19 600 Exemplare**