Vorwort

Als ich im Februar vor 10 Jahren mein erstes Buch zum Thema Cloud Computing herausgegeben habe, führte dieses Segment noch ein Nischendasein. Heute gilt Cloud Computing als Motor der Digitalisierung. Neue Geschäftsmodelle werden durch Cloud-Lösungen erst möglich, mobile Zugriffe auf IT-Ressourcen vereinfacht und eine schnellere Skalierbarkeit der IT-Leistungen erreicht. Cloud Computing wird von den meisten Unternehmen in Anspruch genommen und durch die Pandemie nochmal befeuert. Der Trend geht in Richtung Hybrid und Multi Cloud, um die Vorteile unterschiedlicher Provider und Lösungen für das Unternehmen optimal nutzen zu können.

Auch wenn laut einer repräsentativen Studie des Bitkom Public-Cloud-Lösungen weniger anfällig sind für Sicherheitsvorfälle als die eigene IT im Unternehmen[1], häufen sich mit der zunehmenden Nutzung von Cloud Computing Cyberangriffe. Und auch andere Faktoren stellen ein Sicherheitsrisiko für das Cloud Computing dar – angefangen von technischen Störungen über Fehlkonfigurationen, Datenverlust, mangelnde Awareness der Mitarbeiter bis hin zu Compliance-Verletzungen.

Die Verantwortung für die Sicherheit schultern sowohl die Cloud-Nutzer als auch die Cloud-Anbieter. Als grobe Richtlinie gilt das Prinzip: Der Kunde trägt die Verantwortung für „Security in the Cloud“ und der Cloud-Anbieter für „Security of the Cloud“. Es ist im Sinne beider Parteien, gemeinsam die Sicherheit zu verbessern, um jedwede Folgeschäden abzuwenden.

Durch die Cloud-Nutzung verändert sich die Bedrohungslage, und traditionelle Sicherheitskonzepte und -lösungen wie klassische Anti-Malware-Technologien oder Firewalls lassen sich nicht kurzerhand auf das Cloud-Umfeld übertragen bzw. bieten nicht mehr ausreichenden Schutz. Cloud-Sicherheit erfordert neue Konzepte und hochentwickelte Technologien.

[1] Studie: Cloud-Monitor 2020, S. 26, Bitkom Research im Auftrag von KPMG

Das sind die Themen des Buches:

- Technologischer und organisatorischer Wandel durch Cloud Computing
- Veränderte Bedrohungslage durch Cloud-Nutzung
- Verantwortlichkeiten in der Cloud-Nutzung – das Shared-Responsibility-Modell
- Vorgehensweise zur Cloud-Migration unter sicherheitsrelevanten Aspekten
- Vorgehensmodelle und Umsetzungskonzepte für sichere Hybrid, Public und Multi Clouds
- Sicherheitskonzepte und -maßnahmen der Cloud-Anbieter
- Datenschutz und DSGVO-konforme Datenverschlüsselung
- Umsetzung von Zero-Trust-Architekturen
- Kritische Infrastrukturen: Grundlagen, Anforderungen und sicherheitsrelevante Umsetzungskonzepte
- Best Practices zur automatischen Identifizierung und Behebung von Sicherheitslücken in AWS und in Microsoft Azure

Branchen- und anwendungsbezogene Beispiele aus der Praxis runden das Buch ab.

Das Buch richtet sich an Cloud-Nutzer, die sich auf strategischer, organisatorischer und operationaler Ebene mit den Themen Cloud Computing und IT-Sicherheit auseinandersetzen, aber auch an IT-Dienstleister und Berater sowie Studierende und Dozenten, die Kenntnisse im Umfeld von Cloud Computing erwerben oder vermitteln wollen.

Zwölf hochkarätige Autoren konnten dazu gewonnen werden, sich mit Beiträgen am Gelingen des Buches zu beteiligen. Ihnen gilt mein Dank.

Christiana Köhler-Schute Berlin, im Mai 2021

Inhaltsverzeichnis

Abbildungsverzeichnis:

Tabellen:

Management Abstract

Tino Hirschmann und **Marcel Reviol**, Deutsche Telekom Security, nehmen in ihrem einleitenden Beitrag **Herausforderung Cloud Security: Wandel in Technologie und Organisation** den Leser auf eine kurze Zeitreise mit, um insbesondere jüngeren Lesern den Wandel der IT zu verdeutlichen. Sie geben einführend einen Überblick über Cloud-Services und -Modelle, erläutern das Shared-Responsibility-Modell und beschreiben vier grundsätzliche Vorgehensmodelle zu Anwendungsmigration in die Cloud. Sie stellen auf der Basis von Security by Design sieben Grundregeln auf, die dazu beitragen, die Angriffsfläche von Attacken zu minimieren. Zum Schluss diskutieren sie sicherheitsrelevante Maßnahmen als Reaktion auf eine veränderte Bedrohungslage durch die Cloud-Nutzung und lassen ihre Erfahrungen einfließen.

Die Frage, ob Unternehmen Cloud-Services trauen können, beantworten **Christian Lechner** und **Andreas Schindler**, All for One Group, mit einem klaren „Ja“. Sie stellen in ihrem Beitrag **Der integrierte Ansatz bei der Migration in die Cloud: Security by Default** ihre Vorgehensweise für die Cloud-Migration vor, die auf einer vollständig integrierten Sicherheitsarchitektur beruht. Zur Veranschaulichung ihrer Vorgehensweise berichten sie über ein Cloud-Projekt bei einem Maschinenbauer mit dem Ziel, digitale Produkte schnell entwickeln und bereitstellen zu können. Zum Schluss fassen sie ihre Erfahrungen aus Cloud-Projekten zusammen.

Ralf Stadler, Tech Data, erörtert in seinem Beitrag **Sicher in die Cloud** Maßnahmen und Lösungen zur Sicherung von Anwendungen in Public, Multi und Hybrid Clouds. Zunächst begründet er, warum die im eigenen Rechenzentrum genutzten lokalen Security Tools und Sicherheitskonzepte nicht auf das Cloud-Umfeld übertragen werden können, und welche Maßnahmen ergriffen werden sollten. Er beschreibt verschiedene Lösungen beginnend mit der Authentifizierungslösung RSA SecurID und YubiKey sowie mit der IBM-Lösung IBM Cloud Paks for Security, welche sicherheitsrelevante Informationen über alle Datenquellen, Systeme in einem Hybrid-Multi-Cloud-Umfeld automatisiert zusammenführen und auswerten. Er stellt die Microsoft 365 Business Premium-Lösung und weitere Tools vor, die insbesondere KMUs im Remote-Arbeitsumfeld Schutz bieten.

Dominik Birgelen, oneclick, stellt in seinem Beitrag **Anwendungsbereitstellung über die oneclick™ Cloud-Plattform: Ein schlagkräftiges Mittel gegen Cyberkriminalität** die Cloud-Plattform seines Unternehmens vor, welche als Vermittlungs- bzw. Trennschicht zwischen Benutzer und Unternehmensressource fungiert. Streaming-Server dienen als eine Art Sicherheitsschleuse mit Verschlüsselungen und weiteren Sicherheitsmechanismen zwischen Benutzer und Unternehmensressourcen, unabhängig davon, von wem diese bezogen werden. Inkludiert ist eine Cyberversicherung mit vorgeprüften Sicherheitsmaßnahmen ohne vorherige Fallprüfungen beim Anwenderunternehmen.

„Vertrauen ist gut, Kontrolle ist besser“: Das ist das Motto von Zero Trust. Es sieht vor, dass jede einzelne Anfrage und Zugriffe auf Ressourcen als nicht vertrauenswürdig gelten, bis das Gegenteil bewiesen ist. Mit Auflösung des Perimetersschutzes – als klassischer Ansatz für die Netzwerksicherheit – gilt Zero Trust u.a. im Cloud-Umfeld als ein probates Modell, welches auf großes Interesse stößt. **Michael Doujak**, Ergon Informatik, und **Aarno Aukio**, VSHN, erläutern in ihrem Beitrag **Zero Trust ist eine Reise** ein Migrations-Konzept für die Umsetzung einer Zero-Trust-Architektur in Unternehmen. Sie erörtern die technischen und betrieblichen Vorteile einer Zero-Trust-Architektur, zeigen aber auch die Grenzen von Zero Trust auf. Zur stufenweisen Umsetzung dieser Architektur beschreiben sie ein Modell, welches aus einem API-Gateway aus dem Perimeterschutz – als Aufgabenverteiler zwischen Perimeter und neu eingeführten Microgateways –, Microgateways für den Zero-Trust-Ansatz und einer IAM-Lösung besteht.

Elmar Eperiesi-Beck, eperi, hat den Schwerpunkt seines Beitrages **Datenschutzkonforme Cloud Nutzung – Best Practices für alle Unternehmensgrößen** auf eine datenzentrische Sicht gelegt. „Nicht länger geht es nur um die Sicherheit der Anwendungen. Entscheidend ist der Schutz der darin befindlichen sensiblen Daten“, so der Autor.
Zunächst befasst er sich mit Schutzzielen im Kontext mit Cloud-Computing, die die Sicherheit der IT messbar und die aktuelle Gefahrenlage bewertbar machen. Der Autor erläutert die Sicherheitsmaßnahmen der Cloud-Anbieter, die häufig bereits im Angebot integriert sind oder zugebucht werden können. Zur Beurteilung, ob diese Maßnahmen ausreichend sind, führt er Kriterien an, die es bei der Bewertung zu berücksichtigen gilt. Um den Anforderungen an die Datensicherheit und den Datenschutz gerecht zu werden, plädiert er dafür, die Datenverschlüsselung selbst in die Hand zu nehmen. Er erläutert die verschiedenen Arten der Verschlüsselung und führt zum Schluss mehrere Praxisbeispiele an, die durch den Einsatz von Verschlüsselungslösungen datenschutzgerecht umgesetzt werden konnten.

Kritische Infrastrukturen werden als besonders schützenswürdig eingestuft. Durch die zunehmende Digitalisierung werden die Anlagen und Systeme angreifbarer, und die meldepflichtigen IT-Sicherheitsvorfälle haben im letzten Jahr deutlich zugenommen.
Dr. Simon Woldeab, fuentis, gibt in seinem Beitrag **Herausforderungen für Kritische Infrastrukturen (KRITIS)** zunächst einen Überblick über die derzeitige Gesetzeslage und den entsprechenden Richtlinien. Er listet die KRITIS-Sektoren und Anlagenkategorien sowie die entsprechenden Bemessungsgrundlagen und Schwellenwerte auf und erläutert sie. Er geht auf den Anforderungskatalog des BSI ein und diskutiert das Thema „Stand der Technik" im Zusammenhang mit den branchenspezifischen Sicherheitsstandards (B3S). Zum Schluss veranschaulicht er am Beispiel Krankenhaus den Einsatz eines ISMS unter Einbindung von KRITIS-Standards.

Prof. Dr. Heiko Meyer, KMS Vertrieb und Services, geht in seinem Beitrag **IT-Sicherheit im klinischen Umfeld** darauf ein, warum Kliniksysteme zukünftig als Cloud-Lösung betrieben werden sollten. Er erörtert, warum Hybrid-Cloud-Systeme von Vorteil für Kliniken sind, und gibt Hinweise, wie klinische IT-Systeme sicher in der Cloud betrieben werden können. Dabei werden die gesetzlichen Besonderheiten des Gesundheitswesens näher beschrieben, spezielle Mechanismen zum Schutz der Daten vorgestellt und die daraus resultierenden Vorteile aus betriebswirtschaftlicher und medizinischer Sicht für Patienten, Ärzte, Klinikmanagement sowie Forschung und Wissenschaft erörtert.

Valeri Milke, Insentis, befasst sich in zwei Beiträgen sowohl mit **Best Practices zur automatischen Identifizierung und Behebung der häufigsten kritischen Sicherheitslücken in AWS** als auch mit **Best Practices zur automatischen Identifizierung und Behebung der häufigsten kritischen Sicherheitslücken in Microsoft Azure**. Er legt die Schwerpunkte jeweils auf übergeordnete architektonische Aspekte, auf die wichtigsten sicherheitsbezogenen sowie auf die am häufigsten eingesetzten AWS- und Azure-Services. In tabellarischer Form stellt er den Services detailliert die entsprechenden Handlungsempfehlungen und Maßnahmen gegenüber. Der Autor stellt weitere Tools vor, die die automatisierte Identifizierung von Sicherheitslücken im AWS- und Azure-Umfeld unterstützen. In seinem zweiten Beitrag gibt er zum Abschluss allgemeingültige Hinweise für ein sicheres Cloud Computing.