Datenwächter von morgen: Cloud Security Spezialisten

Geschrieben von Joshua Bucheli, Forscher und Redakteur, in Zusammenarbeit mit Thomas Maurer, Senior Cloud Advocate bei Microsoft und Peter Kosel, Gründer von cyberunity

Im schnell wachsenden Bereich des Cloud Computing sind Cloud Security Spezialisten sehr gefragt. Welche Anforderungen stellen Arbeitgeber an potenzielle Mitarbeitende? Wer sind die grössten Anbieter auf dem Markt und welche Bewerber machen das Rennen? Worin sehen Branchenführer die größten Hürden für Cloud Computing? Und welche Cloud-Sicherheitsspezialisten sind gefragt, um diese Hürden zu bewältigen?

Cloud Computing: ein explodierender Markt

Zwischen 2010 und 2020 wuchs der globale Cloud-Computing-Markt um über 125 Milliarden US-Dollar[1]. So werden heute mehr als 48 % aller Unternehmensdaten in der Cloud gespeichert[2]. Es erstaunt daher kaum, dass ‘die Cloud’ eindeutig zu einer der am schnellsten wachsenden IT-Märkte der Welt gehört.

Dieses Wachstum ist zum Teil auf die jüngst zu beobachtende Veränderung des Mindsets der Unternehmen zurückzuführen: «Der Shift geht dahin, dass die Cloud vermehrt als sichere Lösung anerkannt wird. […] Gerade in den aktuellen COVID-19 Zeiten findet die Cloud verstärkten Zuspruch. Früher war alles was von draussen kam, beziehungsweise

[1] https://www.statista.com/statistics/500541/worldwide-hosting-and-cloud-computing-market/
[2] https://www.statista.com/statistics/1062879/worldwide-cloud-storage-of-corporate-data/

ausserhalb des Unternehmens gespeichert wurde, höchst zweifelhaft – in Zeiten von Homeoffice öffnen sich die Unternehmen. Sie prüfen und implementieren Cloud-Lösungen für 'Zero-Trust Ansätze' » sagt Thomas Maurer, Senior Cloud Advocate bei Microsoft.

Wir speichern unsere Fotos in der Cloud und sehen dort unsere Lieblingssendungen und -filme; wir arbeiten in virtuellen Teams an unseren Spreadsheets, Präsentationen und Textdokumenten in der Cloud; sogar unsere medizinischen und finanziellen Informationen werden vermehrt in der Cloud gespeichert.

Wie bei jeder Technologie gilt auch hier: Je beliebter sie ist, desto wahrscheinlicher ist es, dass sie erhöhten Risiken, beispielsweise durch Cyber-Angriffe, ausgesetzt ist. Ganz speziell das Thema Cloud steht hier im Fokus, da es sich um eine Technologie handelt, die sich mit einem der wertvollsten Güter unserer Zeit beschäftigt: Daten.

Mit der zunehmenden Verbreitung von Cloud Computing steigt also auch der Bedarf an Spezialisten, die in der Lage sind, die Zuverlässigkeit und Sicherheit dieser Plattformen und der darin enthaltenen Daten zu gewährleisten.

Laut Thomas Maurer liegen die Hürden der Unternehmen, sich für eine Cloud-Lösung zu entscheiden zum einem im mangelnden Wissen über Cloud-Lösungen und deren Sicherheit und zum anderen ganz eng damit verbunden das ungute Gefühl, dass die Daten nicht mehr in deren Hoheitsgebiet 'on premise' liegen:

«Unwissenheit führt zu Unsicherheit, damit einher geht auch die Vertrauensfrage: überlasse ich einem externen Dienstleister meine Daten? […] Wie fühlt es sich an, wenn ich meine IT nicht mehr 'anfassen' kann? [...] Wie können Unternehmen die Kontrolle behalten? [...] gerade mit der wachsenden Anzahl an Cyber-Angriffen bewegen wir uns nicht nur in einer komplexen, sondern auch einer äusserst komplizierten Welt.»

Deshalb ist es wichtig, dass sich Unternehmen der Tatsache bewusst werden, dass das Auslagern der am meisten gefährdeten Daten in die Cloud nicht nur die Sicherheit dieser Daten, sondern auch die Sicherheit der verbleibenden On-Premise-Umgebung erhöht, auch wenn dies ein gewisses Mass an Vertrauen erfordert.

Trotz dieser Schwierigkeiten, geht der Trend «definitiv hin zur Cloud» sagt Thomas Maurer. Es wird erwartet, dass die weltweiten Ausgaben für Cloud-Sicherheit im Jahr 2023 12,6 Milliarden Dollar erreichen werden – fast eine Verdoppelung seit 2018[3].

[3] https://www.cybersecurity-insiders.com/by-2023-cloud-security-spending-to-reach-12-6-billion/

Rein monetär werden wir dieses anspruchsvolle Thema nicht in den Griff bekommen. Wenn diese Hürden bewältigt werden sollen, braucht es auch begeisterungsfähige Cloud Security Spezialisten, die nicht nur über technologische Cybersecurity-Kenntnisse, sondern auch über zwischenmenschliche, vor allem kommunikative, Fähigkeiten verfügen.

Marktführer und aufstrebende Unternehmen

Ein immens hoher Bedarf an Cloud Security Spezialisten besteht natürlich bei den Cloud-Lösungsanbietern und Branchenführern wie Amazon Web Services, Google Cloud, Microsoft Azure, Alibaba und IBM. Diese Unternehmen dominieren ihre jeweiligen Märkte und spielen eine wesentliche Rolle bei der Gestaltung der Zukunft des Cloud Computings.

Jedoch sind für Cloud Security Spezialisten auf Seite der Lösungsanbieter auch Engagements bei den Endkunden in allen Branchen sowie bei mittelständischen Cloud-Lösungsanbietern interessant.

Welches Know-how ist bei Cloud Security Spezialisten gefragt?

Bis anhin wurden Cloud-Plattformen oft zuerst entworfen und gebaut und erst dann gesichert. Aber das ändert sich, und Cloud Security Spezialisten, die sich bei Arbeitgebern hervorheben wollen, sollten diesen Wandel erkennen und mitgestalten können.

Datensicherheit im Kontext von Cloud Computing sollte eher ein erster als ein letzter Schritt sein - angehende Cloud Security Spezialisten müssen in der Lage sein, Sicherheitsanforderungen in allen Phasen des Cloud Computing vorauszusehen und proaktiv zu identifizieren, um ein sicheres Design, einen sicheren Aufbau und ein fortlaufendes Sicherheitsmanagement von Cloud-Plattformen zu gewährleisten.

Daher ist es unerlässlich, dass Cloud Security Spezialisten nicht nur die DevOps-Phasen des Cloud Computing beherrschen, sondern auch über die notwendigen Soft Skills verfügen.

Zusätzlich zu diesem ganzheitlichen ‘SecDevOps’-Ansatz sollten angehende Cloud-Sicherheitsspezialisten die wichtigsten Cybersecurity-Konzepte (z.B. die im NIST-Framework enthaltenen Richtlinien), Technologien, Methoden und Best Practices für verschiedene Plattformen, Betriebssysteme und Software kennen.

Sie sollten ein fundiertes Verständnis der verschiedenen Cloud-Lösungen mitbringen - **IaaS**, **PaaS**, **SaaS**, **Public-**, **Private-**, **Hybrid-** und auch **Multi-Cloud** - sowie der jeweiligen sicherheitsrelevanten Fragen, die diese Modelle aufweisen. Eine fundierte Kenntnis der

Analyse von Daten und Machine Learning, wie auch der jeweiligen Sicherheitsrisiken, die mit **Daten im Ruhezustand**, **Daten in Bewegung** und **Daten in Nutzung** verbunden sind, wird ebenfalls dazu beitragen, dass sich angehende Cloud Security Spezialisten von der Konkurrenz abheben.

Sie sollten sich mit dem Design und der Implementierung von **Daten-**, **Netzwerk-**, **Applikations-** und **Container-Sicherheitsmassnahmen** wie **Firewalling**, **Identity-** und **Network- Access Control**, **DdoS-Schutz** usw. auskennen.

Grundsätzlich suchen Cloud-Anbieter natürlich Persönlichkeiten mit einem guten Mix aus technologischem Security-Know-How, Data Privacy-Erfahrung, und Compliance-Wissen, erklärt Thomas Maurer. Jedoch betont er auch die Wichtigkeit dessen, was er 'T-Shaped Learners' nennt – Spezialisten, die über ein breites Wissen verfügen, aber auch zwei bis drei Spezialisierungen (zum Beispiel Cloud-Netzwerksicherheit oder Data Privacy) beherrschen.

Schliesslich sollten diejenigen, die eine Karriere in der Cloud-Sicherheit anstreben, ein grundlegendes Verständnis der **DSGVO**, **ISO 27001**, **DSG** und andere Datenschutz-vorschriften haben, die für ihr jeweiliges Land oder auch international gelten – je nach Internationalisierungsgrad ihres Wirkungsbereichs. Damit sind sie in der Lage, Risiko-bewertungen durchzuführen und die Einhaltung der Vorschriften anlässlich von Audits durch die Behörden nachzuweisen.

Welche Zertifikate sind besonders gefragt?

Zusätzlich zu den herkömmlichen Hochschulabschlüssen in Informatik, sind auch mehrere Zertifizierungen für Sicherheitsspezialisten sehr gefragt. Dies ist besonders wichtig für Quereinsteiger, denen sich auch aussichtsreiche Chancen eröffnen, solange sie ihre Affinität für Informatik in Form einer einschlägigen Grundausbildung abstützen.

«Wichtig ist ein fundiertes IT-Basiswissen, Fokus auf ein Thema und dort tief einsteigen. […] Schau Dir ein Thema an und absolviere das entsprechende Zertifikat wie beispielsweise das AZ-500 Examen für Cloud Security-Engineers und das Azure Security-Engineer Zertifikat» empfiehlt Thomas Maurer.

Die einstellenden IT-Manager bei den Arbeitgebern fragen gerne nach folgenden Zertifikaten: Certificate of Cloud Security Knowledge (**CCSK**), **CompTIA Cloud+** und **CompTIA Cloud Essentials**, Certified Information Systems Auditor (**CISA**), Certified Cloud Security Professional (**CCSP**) und Certified Information Systems Security Professional (**CISSP**).

Soft-Skills: Welche persönlichen Eigenschaften sind gefragt?

Abgesehen von den Hard Skills und Zertifizierungen gibt es für Cloud Security Spezialisten wie auch für alle anderen einige wünschenswerte Soft Skills.

In erster Linie sind zwischenmenschliche Fähigkeiten ein grosses Plus: effektiv und gleichzeitig einfühlsam mit Architekten, Entwicklern, Programmierern und anderen Abteilungen und Teammitgliedern zu kommunizieren, zu überzeugen und zu verhandeln. Die Fähigkeit, Sicherheitsdiagnosen und -lösungen in leicht verständliche Vorträge beim Management, Dokumentationen und Richtlinienempfehlungen zu übersetzen, ist ebenfalls ein erheblicher Vorteil.

Aufgrund der Schnelllebigkeit und der ständigen Weiterentwicklung des Cloud Computing-Marktes sollten Cloud-Sicherheitsspezialisten, die von Arbeitgebern wahrgenommen werden wollen, ihre Dynamik, Innovationsfähigkeit und ihre Neigung zum Querdenken unter Beweis stellen.

Insgesamt wird eine Lifelong-Learning Einstellung geschätzt. Thomas Maurer schlägt vor: immer dran bleiben in der sich schnell verändernden Welt – smart sein und erkennen was gebraucht wird. Authentische Selbstvermarktung ausüben indem man Gutes tut und darüber spricht. Spass daran haben, Know-How weiterzugeben und Wissen mit anderen zu teilen.

Es werden sich die Cloud Security Spezialisten besonders positiv abheben, die Trainings zur Entwicklung der Persönlichkeit aktiv angehen. Ziel ist es die eigene Wirkung zu hinterfragen, um sich auch auf diesem Gebiet, wie auch bei den securityspezifischen Zertifikaten, stetig weiterzuentwickeln.

Schliesslich kann man es kaum besser ausdrücken als Peter Kosel von cyberunity, abschliessend unterstreicht: «Schon alleine die Tatsache, dass sich jemand mit der Wirkung seiner eigenen Persönlichkeit in Form einer Weiterbildung auseinandersetzt zeugt von einer sehr offenen, lernfreudigen und vor allem positiven Haltung. Und Haltung entscheidet.»