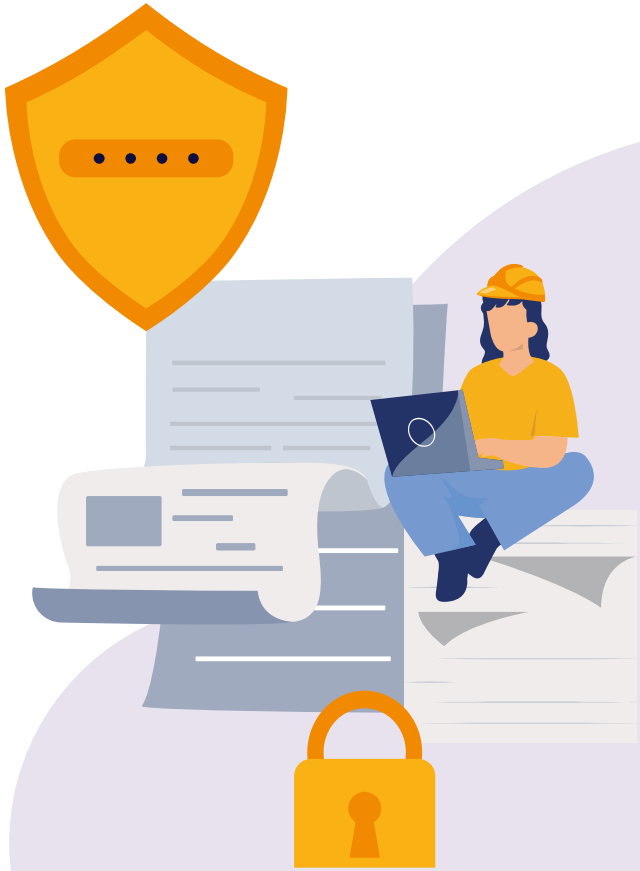
Cloud Security – individuelle Risiken und effektive Maßnahmen

Von Jens Westphal

Die Migration in die Cloud ist für zahlreiche Unternehmen ein entscheidender Schritt auf dem Pfad der digitalen Transformation. Sie birgt viele Vorteile, konfrontiert uns jedoch gleichzeitig mit einer Reihe von Herausforderungen. Um diese erfolgreich zu bewältigen, ist es von grundlegender Bedeutung, sämtliche Risiken und Bedrohungen individuell abzuwägen und geeignete Maßnahmen zu ergreifen.

In einer Welt, die immer stärker auf Technologie setzt und insbesondere die Cloud-Technologie favorisiert, nimmt die Relevanz des Themas Cybersicherheit unaufhörlich zu. Dieser Aspekt und die schwer einzuschätzenden Risiken bewegen einige Unternehmen jedoch immer noch dazu, vor dem großen Sprung in die Cloud zurückzuschrecken. Im Zentrum ihrer Bedenken stehen dabei Datensicherheit, Datenschutz und Compliance-Anforderungen, denn die Dezentralisierung von Daten kann Unsicherheit erzeugen.

Die Cloud bietet bei Sicherheitsaspekten Vorteile, aber auch Herausforderungen. Für bestimmte Bedrohungsarten entstehen Vorteile, dafür kommen neue Bedrohungsarten hinzu. Dabei gilt es, verschiedene Dimensionen und Szenarien zu betrachten. Die spezifischen Herausforderungen bei der Implementierung von Cloud-Diensten variieren in Abhängigkeit von der Art der durch Unternehmen verarbeiteten Daten, der Unternehmensgröße, der Branche und vielen weiteren Faktoren. So gehen stark regulierte Branchen oftmals mit sensiblen und vertraulichen Daten um, die einen besonderen gesetzlichen Schutz haben. Hier führen beispielsweise spezifische Branchenvorgaben zu strikten Compliance-Anforderungen, die in der Cloud-Umgebung neue Herausforderungen nach sich ziehen. Gefragt sind eine durchdachte Sicherheitsstrategie und eine gut geplante Umsetzung.



Unternehmensspezifische Herausforderungen bei der Cloud-Implementierung

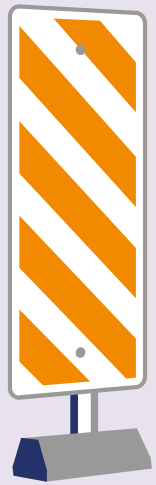
Die Frage „Wie sicher ist die Cloud?“ wird oftmals zu allgemein und zu pauschal beantwortet. Aussagekräftiger ist die Diskussion der Frage: Was kann einem Unternehmen bei einem Angriff tatsächlich passieren? Entscheidend ist, welche Daten und Anwendungen in der Cloud verarbeitet werden und welchen Wert sie für Dritte haben. Ein einfaches Beispiel aus dem täglichen Leben könnte eine Gartenhütte sein, in der lediglich alte Gartengeräte lagern. Hier genügt ein einfaches Schloss zur Absicherung. Anders ist es, wenn in der Hütte Goldbarren aufbewahrt werden. Hier muss man sicherlich stärkere Schutzmaßnahmen ergreifen. Analog dazu müssen in der Cloud gespeicherte Daten und Anwendungen je nach Wichtigkeit und Sensibilität unterschiedlich geschützt werden.

Unbestreitbare Vorteile bietet die Cloud in Bezug auf die Verfügbarkeit und Wiederherstellbarkeit von Systemen. Wenn beispielsweise im klassischen Falle des eigenen Rechenzentrums nach einem erfolgreichen Angriff der gesamte Hardwarebestand als nicht mehr vertrauenswürdig angesehen werden muss, da jedes betroffene System und jeder Server kompromittiert und damit ein potentielles dauerhaftes Risiko darstellen könnte, stünde das Unternehmen vor der gewaltigen Aufgabe, seine IT-Infrastruktur vollständig neu aufzubauen. Das ist sowohl zeitaufwendig als auch kostenintensiv. Lägen alle Systeme in der Cloud, könnte das Unternehmen agiler und effizienter handeln. Das infizierte System in der Cloud ließe sich einfach abschalten und neu aufbauen – eine wesentlich kostengünstigere Lösung im Vergleich zum Neuaufbau einer physischen IT-Infrastruktur. Darüber hinaus kann eine rasche Wiederherstellung des Betriebs nach einem Angriff den Schaden begrenzen und die Ausfallzeit minimieren.

Bedrohungsanalyse als Ausgangspunkt für die Risikobewertung

Cloud-Sicherheit erfordert eine kontinuierliche Risikobewertung und Maßnahmenanpassung, um mit der dynamischen Bedrohungsentwicklung Schritt zu halten. Nur so kann ein Unternehmen die Vorteile der Cloud nutzen, ohne dabei seine Daten und Systeme zu gefährden. Jedes Unternehmen muss zusätzlich zu den Standard-Sicherheitsmaßnahmen der Cloud-Dienste immer eine eigene, auf das individuelle Unternehmen zugeschnittene Risikobewertung durchführen sowie eine eigene Sicherheitsstrategie entwickeln und umsetzen.

Ein Risiko entsteht grundsätzlich immer dann, wenn eine Bedrohung auf eine Schwachstelle trifft. Da sich die Bedrohungen stetig verändern und ständig neue Schwachstellen aufgedeckt werden, ist ein kontinuierlicher Prozess zur Risikominimierung erforderlich. Zur Bewertung der Bedrohungslage muss daher jeder Bedrohungsvektor einzeln anhand der Anforderungen und der Situation des jeweiligen Unternehmens und seiner IT-Infrastruktur bewertet werden. Während traditionell in der IT-Sicherheit die Hauptbedrohungen im Bereich der physischen und netzwerkbasierten Sicherheit liegen, verändert die Migration in die Cloud diese Bedrohungsvektoren. Die physische Absicherung von Serverräumen liegt nun hauptsächlich beim Cloud-Anbieter. In den Fokus der Risikobewertung rücken stattdessen Bereiche wie Zugriffskontrolle und Identitätsmanagement, Datenverschlüsselung, sicheres Design und die Konfiguration von Cloud-Diensten.



Der Weg zu einer ausgewogenen Risikobewertung

Der Prozess zur Erstellung einer ausgewogenen Risikobewertung für die Nutzung von Cloud-Umgebungen erfordert ein systematisches Vorgehen. Ziel ist es, ein Gleichgewicht zwischen den geschäftlichen Vorteilen der Cloud und potenziellen Sicherheitsrisiken zu finden. Dies erfordert die Zusammenarbeit verschiedener Spezialisten, etwa eines Cloud-Architekten und eines Sicherheitsspezialisten. In der Praxis beginnt der Prozess mit einer Bestandsaufnahme der bestehenden IT-Systeme und einer Einschätzung, welche davon in die Cloud migriert werden sollten. Daraufhin modelliert der Cloud-Architekt, der einen umfassenden Überblick über die gesamte IT-Landschaft besitzt, eine Zielarchitektur. Parallel dazu wird ein Cloud-Security-Spezialist hinzugezogen, der die potenziellen Bedrohungsvektoren in der geplanten Architektur und während des Transformationsprozesses identifiziert und daraus entsprechende Sicherheitsmaßnahmen ableitet.

Dieser Prozess erinnert an den Bau eines Hauses, bei dem Architekten und Statiker zusammenarbeiten. Der Cloud-Security-Spezialist hat eine ähnliche Funktion wie ein Statiker beim Hausbau. Er muss verstehen, wie bestimmte Elemente miteinander interagieren und wo Anpassungen erforderlich sind. Seine Expertise und Kenntnisse, zum Beispiel in Bezug auf Methoden und Standards wie C5 oder Mobile Office Records, sind entscheidend, um die Sicherheitsstruktur zu optimieren. So wie ein erfahrener Statiker baufällige Strukturen identifizieren und verbessern kann, bevor das Risiko eines Einsturzes entsteht, hat ein Cloud-Security-Spezialist Erfahrung mit problematischen Sicherheitsszenarien. Mit den vom Sicherheitsspezialisten erarbeiteten Informationen kann der Cloud-Architekt dann entscheiden, wie beispielsweise das „Prinzip Zero Trust“ oder andere Sicherheitsmechanismen umgesetzt werden. Das ausgearbeitete Sicherheitskonzept wird schriftlich festgehalten, detailliert beschrieben und kann als Referenz und für Prüfungen und Audits herangezogen werden.

Umsetzung der Migration in die Cloud

Anschließend wird die Cloud-Umgebung aufgebaut und eine Prüfung durchgeführt, um sicherzustellen, dass alles wie im Sicherheitskonzept beschrieben umgesetzt wurde. Ähnlich wie bei einem Hausbau kann ein externer Prüfer das Konzept bestätigen und eine Art „Baugenehmigung“ erteilen. Nach Abschluss der Prüfung und Bereitstellung der Cloud-Umgebung wird die Migration durchgeführt. Dabei ist die Reihenfolge, in der die Dienste eingeführt werden, entscheidend. Spezialisierte Dienstleistungen, wie das „Security Incident Event Management“ (SIEM), spielen in diesem Kontext eine wichtige Rolle. SIEM-Systeme bieten Echtzeit-Analysen von sicherheitsrelevanten Vorkommnissen und Log-Daten, die von Netzwerkhardware und -anwendungen generiert werden. Sie helfen dabei, irregulären Betrieb zu erkennen und rechtzeitig zu reagieren. Allerdings erfordert die Überwachung dieser Systeme qualifizierte Expertise. Unternehmen benötigen daher entweder interne Spezialisten oder externe Dienstleistungen, um die Funktionsfähigkeit der Sicherheitssysteme ständig gewährleisten zu können.

Die Bedeutung von Sicherheit nach der Migration

Weitere fortlaufende Dienstleistungen umfassen regelmäßige technische Analysen, Penetrationstests, Organisationsanalysen und Audits, um sicherzustellen, dass das implementierte System dauerhaft funktioniert und an die sich ständig ändernde Bedrohungslage angepasst wird. Dabei ist es wichtig, dass die Dienstleistungen zu den Geschäftszielen und Bedürfnissen des Unternehmens passen. Ein effektiver Schutz muss dabei auch wirtschaftlich sein. Daher sollte die Dimensionierung der Sicherheitsziele immer so erfolgen, dass sie erreicht werden können, ohne die finanzielle Stabilität des Unternehmens zu gefährden.

Ein entscheidender Faktor in diesem Prozess ist das Vertrauen. Die Unternehmen müssen darauf vertrauen können, dass IT-Sicherheitsdienstleister die Interessen des Unternehmens im Blick haben und dass sie die geschäftlichen Aspekte ebenso verstehen wie die technischen. Dieser Vertrauensaufbau durch ein tiefes Verständnis des Geschäfts und die Bereitstellung effektiver, wirtschaftlich sinnvoller Lösungen kann letztlich den Grundstein für langjährige, produktive Zusammenarbeit legen.

Cybersicherheit: Bleiben Sie dran!

In der sich stetig wandelnden digitalen Landschaft sind eine robuste Cloud-Sicherheitsstrategie, eine sorgfältige Umsetzung und regelmäßige Überprüfungen nicht mehr nur wünschenswert, sondern unumgänglich. Gleichzeitig benötigen wir einen kulturellen Wandel, der die Bedeutung von Datensicherheit in der Cloud verankert.

Während wir uns in eine neue Ära der Cloud-Sicherheit bewegen, geprägt durch technologische Innovationen und ein gesteigertes Nutzerbewusstsein, erinnert uns der ständige Fortschritt daran, dass wir kontinuierlich anpassungsfähig und lernbereit sein müssen. Denn Cloud-Sicherheit ist kein statisches Ziel, sondern eine dynamische Herausforderung, bei der wir stets bestrebt sein müssen, einen Schritt voraus zu sein, damit die Cloud ein sicherer und vertrauenswürdiger Ort für all unsere digitalen Bedürfnisse ist und bleibt.