Digital Business University of Applied Sciences

Cyber- & IT-Security (M.Sc.)

Cloud Computing & Cloud Security

Wintersemester 2024/25

Betriebswirtschaftliche Faktoren

Aufgabe 3

Eingereicht von:
Elias Häussler

Matrikelnummer:
200094

Dozent:
Prof. Dr. Aymen Gatri

17. April 2025

Aufgabe

Diskutiere ausführlich, inwieweit betriebswirtschaftliche Faktoren eine Rolle bei Informationssicherheitsentscheidungen spielen. Folgende Punkte solltest du diskutieren:

- Wieso können Cloud-Dienste im Allgemeinen einen Beitrag zur Wirtschaftlichkeit leisten?
- Welche Kosten müssen bei Cloud-Diensten immer beachtet werden?
- Welche anderen Mechanismen neben dem *Return on Security Investment* gibt es?
- Gibt es regulatorische Risiken oder Einschränkungen beim Einsatz von Cloud-Diensten?

Wirtschaftliche Überlegungen zur Vereinbarkeit von Cloud Computing und Informationssicherheit

Wenn Unternehmen entscheiden, einzelne Dienste oder Bereiche ihres Geschäftsbetriebs in die Cloud auszulagern, müssen sie sorgfältig abwägen, ob die damit verbundenen Vorteile mit den Anforderungen an die Informationssicherheit vereinbar sind. Cloud Computing kann betriebswirtschaftlich mit erheblichen Kosteneinsparungen einhergehen, birgt jedoch auch Risiken, insbesondere im Hinblick auf die sichere Verarbeitung, Speicherung und Weitergabe von Daten. Ein ausgewogenes Verhältnis von Risiko, Nutzen und Kosten ist notwendig, damit Cloud Computing und Informationssicherheit miteinander vereinbar und zugleich wirtschaftlich effizient bleiben.

Cloud-Dienste im Kontext von Wirtschaftlichkeit

Um zu verstehen, warum Cloud-Dienste einen wesentlichen Beitrag zur Wirtschaftlichkeit leisten können, ist es sinnvoll, zunächst die damit verbundenen Kostenfaktoren zu betrachten.

Kostenfaktoren bei Cloud-Diensten

Bei der Überführung eines bestehenden Systems in die Cloud entstehen in der Regel Kosten für die Datenmigration. Diese variieren je nach Zustand und Umfang des bestehenden Systems, etwaigen Unterschieden zwischen alter und neuer Umgebung, der Notwendigkeit einer Ausfallsicherheit während der Migration, möglichen nachträglichen Migrationen veränderter Daten sowie dem Aufwand für die Entwicklung geeigneter Backup- und Wiederherstellungsstrategien.

Bei der Neuinstallation eines Cloud-Dienstes entfallen Migrationskosten in der Regel. Dennoch ist es gerade bei der Einführung eines neuen Dienstes essenziell, dass dieser zu Beginn umfassend getestet und für den produktiven Betrieb vorbereitet wird. Besonders wichtig ist beim Cloud Computing die Implementierung effizienter Backup-Prozesse und Sicherheitsmaßnahmen wie Verschlüsselung oder Identitätsmanagement, da die Datenverarbeitung nicht mehr ausschließlich durch das Unternehmen selbst, sondern auch durch den Cloud-Anbieter erfolgt.

Auch regulatorische Anforderungen, etwa aus der Erfüllung gesetzlicher Vorgaben wie der DSGVO[1], müssen beim Betrieb von Cloud-Diensten berücksichtigt werden. Sie sind meist mit zusätzlichen Kosten verbunden und stellen einen betriebswirtschaftlich nicht zu vernachlässigenden Faktor dar. Diese Kosten lassen sich reduzieren, wenn ein Cloud-Anbieter gewählt wird, der die entsprechenden Anforderungen bereits erfüllt.

[1] Datenschutz-Grundverordnung

Cloud Computing als Beitrag zur Wirtschaftlichkeit

Die Nutzung von Cloud-Diensten ist zweifellos mit Kosten verbunden. Verglichen mit klassischen IT-Infrastrukturen können sie jedoch als Effizienztreiber betrachtet werden und bieten darüber hinaus eine Vielzahl an Vorteilen.

Ein wesentlicher Faktor ist die Möglichkeit großer Cloud-Anbieter, IT-Ressourcen zu deutlich geringeren Kosten bereitzustellen, als dies für einzelne Unternehmen beim Eigenbetrieb möglich wäre. Durch den Betrieb großer Rechenzentren können Ressourcen in einem Umfang bereitgestellt werden, der eine signifikante Kosteneffizienz ermöglicht.

Darüber hinaus bietet Cloud Computing eine kostengünstige und bedarfsgerechte Skalierbarkeit. Das Anmieten von Serverressourcen bei einem Cloud-Anbieter ist in der Regel deutlich wirtschaftlicher als der Ausbau eigener IT-Infrastrukturen, der nicht nur mit Hardwarekosten, sondern auch mit zusätzlichen Aufwänden in Wartung, Betrieb und Sicherheit einhergeht. Gerade im Bereich der Informationssicherheit wird Skalierung zur Herausforderung: Zugriffskontrollen, der Aufbau robuster Abwehrmechanismen und die Sicherstellung kontinuierlicher Verfügbarkeit bei wachsender Infrastruktur sprechen auch aus betriebswirtschaftlicher Sicht für den Betrieb in der Cloud.

Auch die flexible Skalierung ist ein bedeutender Kostenfaktor. Bei kurzfristigen Lastspitzen oder temporären Projekten lässt sich eine skalierte Cloud-Infrastruktur meist ebenso kurzfristig wieder zurückfahren – ein Vorteil, den klassische Infrastrukturen kaum bieten können. Einmal angeschaffte Hardware kann nicht ohne Weiteres wieder veräußert oder anderweitig genutzt werden.

Dynamische Skalierbarkeit und Flexibilität im Cloud Computing bieten somit einen deutlichen Vorteil gegenüber unflexiblen und kostenintensiven Überkapazitäten traditioneller IT-Infrastrukturen. Auch die im Cloud-Umfeld etablierte *Pay-per-Use*-Strategie ist hierbei erfolgsentscheidend: Unternehmen zahlen nur für tatsächlich genutzte Ressourcen und profitieren dadurch von einer bedarfsgerechten Abrechnung. Dies ermöglicht zudem eine signifikante Reduktion der Investitionsausgaben (CAPEX[2]).

Metriken zur Messbarkeit erfolgreicher Sicherheitsinvestitionen

Investitionen in Informationssicherheit sind ein zentraler Bestandteil unternehmerischer Ausgaben, insbesondere wenn es darum geht, deren Erfolg messbar zu machen. Neben dem allgemein gebräuchlichen ROI[3] wurde mit dem ROSI[4] eine spezifische Kennzahl entwickelt, die sich auf die Bewertung von Sicherheitsinvestitionen konzentriert.

Der ROSI ist jedoch nur eine von mehreren Möglichkeiten zur Erfolgsmessung. Während sein Fokus vor allem auf der klassischen Kapitalrendite liegt, kann auch eine ganzheitlichere Betrachtung sinnvoll sein. Hierbei sollte insbesondere der potenzielle wirt-

[2] Capital expenditure
[3] Return on Investment
[4] Return on Security Investment

schaftliche Schaden durch Sicherheitsvorfälle systematisch quantifiziert werden. Diese Bewertung umfasst sowohl direkte als auch indirekte Kosten – etwa durch Betriebsunterbrechungen, Reputationsverluste oder rechtliche Konsequenzen. Die Messbarkeit ergibt sich dabei aus dem Vergleich potenzieller Verluste mit den tatsächlich getätigten Sicherheitsinvestitionen, etwa im Rahmen einer CBA[5] (Legato Security, 2024).

Eine weitere relevante Metrik ist der VaR[6], mit dem sich potenzielle Verluste durch Sicherheitsbedrohungen quantifizieren und auf dieser Grundlage fundierte Investitionsentscheidungen treffen lassen. Ursprünglich aus dem Finanzwesen stammend, lässt sich das Konzept auch auf die Informationssicherheit übertragen. Der VaR kombiniert den erwarteten Verlust mit der Eintrittswahrscheinlichkeit und -häufigkeit und adressiert damit drei zentrale Herausforderungen: Sicherheitsmaßnahmen generieren keinen direkten Umsatz, ihr Nutzen ist häufig nicht unmittelbar sichtbar und ohne standardisierte Methoden fällt die Priorisierung einzelner Maßnahmen schwer. Die VaR-Metrik setzt hier an, indem sie Risiken in finanziellen Begriffen ausdrückt und so eine verlässliche Grundlage für Investitionsentscheidungen schafft (Bolloju, 2024).

Regulatorische Risiken & Einschränkungen

Die Kosten, die durch die Erfüllung gesetzlicher Vorgaben wie der DSGVO entstehen, sind nur ein Aspekt der regulatorischen Herausforderungen im Cloud Computing. Datenschutz und die Verarbeitung personenbezogener Daten stellen hierbei ein besonders sensibles Thema dar. Es ist sicherzustellen, dass die Verarbeitung rechtmäßig erfolgt und die Grundsätze der DSGVO konsequent eingehalten werden. Dabei muss der Cloud-Anbieter, wie jeder beteiligte Auftragsverarbeiter, einen AVV[7] unterzeichnen, der seine Maßnahmen zur Einhaltung regulatorischer Anforderungen dokumentiert.

Besonders kritisch ist die Übermittlung personenbezogener Daten in Drittländer. Unternehmen mit Sitz in der EU, die Cloud-Dienste außerhalb des europäischen Wirtschaftsraums nutzen, sind verpflichtet, geeignete Garantien zum Schutz der Daten zu treffen. Die DSGVO stellt in diesem Zusammenhang hohe Anforderungen. Darüber hinaus müssen ggf. weitere nationale und internationale gesetzliche Vorgaben berücksichtigt werden. Der grenzüberschreitende Datenverkehr ist daher mit erheblichen Risiken und Einschränkungen verbunden.

Hinzu kommen branchenspezifische Anforderungen und Nachweispflichten. Besonders Unternehmen im Bereich kritischer Infrastrukturen oder im Gesundheitswesen unterliegen strengen regulatorischen Vorgaben. Die Einhaltung dieser Vorschriften muss häufig durch Zertifizierungen und regelmäßige Audits nachgewiesen werden. Bei Verstößen drohen empfindliche Sanktionen – sowohl in Form finanzieller Strafen als auch durch Reputationsverluste.

[5] Cost-benefit analysis
[6] Value at Risk
[7] Auftragsverarbeitungsvertrag

Literaturverzeichnis

Bolloju, S. (2024). Value at Risk(VaR): A Strategic Approach to Cybersecurity Investments [Online; abgerufen am 15. April 2025]. https://www.linkedin.com/pulse/value-riskvar-strategic-approach-cybersecurity-sateesh-bolloju-myurc/

Legato Security. (2024). Quantifying the Cost of Cybersecurity Risks vs. Investments [Online; abgerufen am 15. April 2025]. https://www.legatosecurity.com/blog/quantifying-the-cost-of-cybersecurity-risks-vs-investments

Eigenständigkeitserklärung

Ich trage die Verantwortung für die Qualität des Textes sowie die Auswahl aller Inhalte und habe sichergestellt, dass Informationen und Argumente mit geeigneten wissenschaftlichen Quellen belegt bzw. gestützt werden. Die aus fremden Quellen direkt oder indirekt übernommenen Texte, Gedankengänge, Konzepte, Grafiken usw. in meinen Ausführungen habe ich als solche eindeutig gekennzeichnet und mit vollständigen Verweisen auf die jeweilige Quelle versehen. Alle weiteren Inhalte dieser Arbeit (Textteile, Abbildungen, Tabellen etc.) ohne entsprechende Verweise stammen im urheberrechtlichen Sinn von mir.

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Alle sinngemäß und wörtlich übernommenen Textstellen aus fremden Quellen wurden kenntlich gemacht.

Die vorliegende Arbeit wurde bisher weder im In- noch im Ausland in gleicher oder ähnlicher Form einer anderen Prüfungsbehörde vorgelegt.

Erklärung zu (gen)KI-Tools

Verwendung von (gen)KI-Tools

Ich versichere, dass ich mich (gen)KI-Tools lediglich als Hilfsmittel bedient habe und in der vorliegenden Arbeit mein gestalterischer Einfluss überwiegt. Ich verantworte die Übernahme jeglicher von mir verwendeter Textpassagen vollumfänglich selbst. In der Übersicht verwendeter (gen)KI-Tools habe ich sämtliche eingesetzte (gen)KI-Tools, deren Einsatzform sowie die jeweils betroffenen Teile der Arbeit einzeln aufgeführt. Ich versichere, dass ich keine (gen)KI-Tools verwendet habe, deren Nutzung der Prüfer bzw. die Prüferin explizit schriftlich ausgeschlossen hat.

Hinweis: Sofern die zuständigen Prüfenden bis zum Zeitpunkt der Ausgabe der Aufgabenstellung konkrete (gen)KI-Tools ausdrücklich als nicht anzeige-/kennzeichnungspflichtig benannt haben, müssen diese nicht aufgeführt werden.

Ich erkläre weiterhin, dass ich mich aktiv über die Leistungsfähigkeit und Beschränkungen der unten genannten (gen)KI-Tools informiert habe und überprüft habe, dass die mithilfe der genannten (gen)KI-Tools generierten und von mir übernommenen Inhalte faktisch richtig sind.

Übersicht verwendeter (gen)KI-Tools

Die (gen)KI-Tools habe ich, wie im Folgenden dargestellt, eingesetzt.

(gen)KI-Tool	**Einsatzform**	**Betroffene Teile der Arbeit**
ChatGPT	Generierung von Zusammenfassungen verschiedener Literaturwerke	Gesamte Arbeit

Münster, 17. April 2025

Elias Häußler