

Zehn Regeln für Cloud Security – Experton Group erstellt Handlungsleitfaden

- **Risikomanagement, Service Level Agreements und Provider Management sind Basis für solide Cloud Security**
- **Anbieter von Cloud Services müssen dringend Sicherheits-Standards schaffen und kommunizieren**
- **Experton Group unterstützt mit Handlungsleitfaden für Cloud Security**

Cloud Services sind in aller Munde, doch wie steht es um die Sicherheit dieser Dienste? Die Diskussion wird heute oftmals auf technologischer Ebene geführt, doch der wahre Schlüssel zum Erfolg liegt in den Aktivitäten rund um Risikoanalysen, Service Level Agreements und Provider Management. Dann lässt sich durch extern bezogene Cloud Services mit vertretbarem Aufwand ein höheres Sicherheitsniveau als bei der Inhouse-Variante erzielen.

Immer mehr deutsche Unternehmen prüfen extern angebotene Cloud Services. Als Hemmnis für deren Einsatz werden aber immer wieder Sicherheitsbedenken und Compliance-Aspekte ins Feld geführt. Ausgenommen hiervon sind einzelne Dienste, die schon einige Jahre am Markt platziert und erprobt sind.

„Die Situation erscheint paradox: grundsätzlich ermöglichen es externe Cloud Services der Mehrzahl der Kunden, die Sicherheit bestimmter Anwendungen und Dienste auf ein höheres Niveau als bislang zu heben“ sagt Wolfram Funk, Senior Advisor bei der Experton Group. „Da externe Cloud-Dienstleister ihre Dienste für eine Vielzahl von Kunden anbieten, verfügen sie über die Skaleneffekte, die hohe Investitionen in eine hochsichere Infrastruktur erlauben.“

Solide technische Maßnahmen zur Absicherung von Cloud Services sind wichtig und bereits heute überwiegend einsetzbar. Noch wichtiger jedoch ist die Ausgestaltung der Beziehung zum Cloud-Dienstleister und den damit verknüpften Aktivitäten, die den Rahmen für die technologische Ausgestaltung prägen. „Risikoanalysen, Service Level Agreements und Provider-Management sind mit Blick auf Cloud Security der Schlüssel zum Erfolg“, stellt Wolfram Funk fest. Die ISO 2700x-Reihe, BSI IT-Grundschutz und ITIL geben hierfür einen geeigneten Rahmen vor.

Dies sind die zehn Regeln für eine hohe Sicherheit von extern bezogenen Cloud Services:

1. Zunächst die interne Organisationsstruktur auf Vordermann bringen sowie Verantwortlichkeiten und Rollen für Informationssicherheit intern klären. Dies gilt auch für das Informationssicherheits-Management und die Steuerung (Governance) von Informationssicherheit.
2. Die Verantwortung für Informations-Sicherheit insgesamt und für Koordination, Management und Qualitätskontrolle externer Dienstleister verbleibt immer im Unternehmen – auch bei extern bezogenen Cloud Services.

3. Eine detaillierte Risikoanalyse für den spezifischen Cloud Service, der extern bezogen wird, sowie die zur Debatte stehenden Informationen und Prozesse durchführen. Dies schließt Compliance-Risiken mit ein.
4. Ist der Business Case stimmig? Wirtschaftliche Aspekte, interne und kundenorientierte Prozessverbesserungen und weitere potenzielle Nutzeneffekte müssen den erwarteten (Rest-) Risiken gegenübergestellt werden.
5. Sicherheitsarchitektur: Arbeitsteilung und Schnittstellen zwischen dem Provider und dem eigenen Unternehmen detailliert festlegen. Sind die technischen und organisatorischen Sicherheitsmaßnahmen lückenlos?
6. Prozesse für Reporting, Incident Management und Audits beim Dienstleister festschreiben.
7. Kann der Cloud-Dienstleister die angeforderte Leistung auch tatsächlich erbringen? Hier ist auch zu hinterfragen, ob er Subunternehmer einsetzt, die zu einer (negativ) veränderten Risikoexposition führen könnten.
8. Die Einhaltung regulatorischer Anforderungen durch den Provider klären und festschreiben, u.a. mit Blick auf den Umgang mit Daten und deren Speicherung in bestimmten Regionen.
9. Für sicherheitsrelevante Kriterien sollen nur solche Service Level vereinbart werden, die gemessen werden können. Die vorgeschlagene Messmethode muss sorgfältig geprüft werden.
10. Der Kunde muss im Vorfeld festlegen, wie die Exit-Bedingungen im Falle eines Providerwechsels aussehen. Ein „Vendor-Lock-In“ kann das Unternehmen im Ernstfall teuer zu stehen kommen.

Zehn Regeln für Cloud Security

Outsourcing-Szenario



1. Management von Informationssicherheit (IS) intern sauber aufsetzen
2. Die Verantwortung für IS und Provider-Management bleibt im Unternehmen
3. Risikoanalyse für den Cloud Service und relevante Prozesse / Informationen
4. Business Case definieren und prüfen
5. Sicherheitsarchitektur, Schnittstellen und Schnittstellen zum Provider klären
6. Prozesse für Reporting, Incident Management und Audits abstimmen
7. Leistungsfähigkeit des Cloud-Service-Anbieters / seiner Sublieferanten prüfen
8. Compliance-Anforderungen klären und in SLAs regeln
9. Nur messbare Kriterien in Service Levels festschreiben
10. Exit-Bedingungen im Vorfeld regeln

www.experton-group.de

Abbildung 1: Zehn Regeln für Cloud Security

Wie aufwändig die Prozesse rund um Cloud Security werden, hängt vom spezifischen Dienst ab. Tendenziell erlaubt es das SaaS-Modell (Software as a Service) am ehesten, mit überschaubarem Aufwand ein hohes Sicherheitsniveau zu erreichen. Bei SaaS ist die Schnittstelle zwischen Provider und Kunde in der Regel sehr gut beschrieben, da der Zugriff über einen Webbrowser erfolgt und für die Verschlüsselung der Übertragungsstrecke SSL/TLS als Standard gesetzt ist. Der Anbieter kümmert sich komplett um die Sicherheitsmaßnahmen in seiner Cloud-Infrastruktur. Allerdings sollten im Vorfeld unbedingt Fragen rund um Compliance, Reporting und Auditierung aus der SaaS-Anwendung heraus sowie Backup und e-Discovery geklärt werden. Außerdem müssen die Anforderungen an das Identitäts- und Zugriffsmanagement beim Kunden eingehend geprüft werden.

Schwieriger wird es bei PaaS (Platform as a Service) oder gar IaaS (Infrastructure as a Service). Dort werden höhere Anforderungen an die detaillierte Festlegung der Arbeitsteilung zwischen Kunde und Anbieter gestellt, was das Thema Informationssicherheit angeht. Unternehmen, die wenig Erfahrung mit Outsourcing allgemein und speziell auch mit Blick auf den zur Debatte stehenden Service haben, sollten einen kompetenten Sourcing- und Sicherheitsberater hinzuziehen.

„Die Anbieter von Cloud Services müssen heute die Standards für Cloud Security aktiv mitgestalten und dafür sorgen, dass anbieterübergreifend ein hohes Sicherheitsniveau erreicht wird“, fordert Wolfram Funk. Sie sollten großes Augenmerk auf vertrauensbildende Maßnahmen bei den künftigen Kunden legen und vor allem mehr Transparenz in den Cloud-Service-Angeboten schaffen.

Die Experton Group bietet interessierten Unternehmen auf Anfrage einen Handlungsleitfaden mit Empfehlungen und Checklisten für Cloud Security Governance, Compliance und technische Sicherheitsmaßnahmen.

Wolfram Funk ist bei der Experton Group AG als Senior Advisor tätig.

Herrn Funks Schwerpunkt liegt in der Beratung von ICT-Dienstleistern, –Herstellern und Telekommunikations-Dienstleistern mit Blick auf Marktforschung und Go-To-Market-Strategien. Wichtige Fokus-Themen von Herrn Funk sind Informationssicherheit, Mobile Computing und ICT-Konvergenz. Außerdem berät Wolfram Funk Anwenderunternehmen mit Blick auf Security- und Risikomanagement sowie das Sourcing von Sicherheitslösungen und -dienstleistungen.



Vor seinem Wechsel zur Experton Group AG im Jahr 2005 war Wolfram Funk bei der META Group Deutschland GmbH als Senior Consultant im Bereich Vendor Consulting beschäftigt. Von 1997 bis 1999 war Herr Funk bei der Xcc Software AG in Vertrieb und Marketing tätig. Dort zeichnete er sich unter anderem mitverantwortlich für die strategische Marktforschung sowie die Konzeption und Umsetzung der Marketingstrategie des mittelständischen IT-Dienstleisters.

Wolfram Funk besitzt einen Abschluss als Diplom-Wirtschaftsingenieur der Universität Karlsruhe (TH) und ist Certified Information Security Manager (CISM, ISACA).

Kontakt: wolfram.funk@experton-group.com