#SURVIVEANDPROSPER

Richtlinie zur Nutzung von Cloud-Diensten

Anforderungen an die sichere Nutzung von Cloud-Diensten

Zusammenfassung	Klicken Sie hier, um Text einzugeben.

Managementsystem	ISMS-Dokument
Dokument-Nr.	IS-K5-00
Version	**v**Klicken Sie hier, um Text einzugeben.
Datum	**07.10.2019**
Status	in Bearbeitung
Klassifizierung	**Vertraulich**

Dokument-Betreuer	Klicken Sie hier, um Text einzugeben. | Klicken Sie hier, um Text einzugeben.
Dokument-Organisation	Klicken Sie hier, um Text einzugeben.
Dokument-Typ	Dokumentvorlage
Zentralisierung	Zentrales Dokument mit lokaler Anpassung (ZLD)
Ablagepfad	

#SURVIVEANDPROSPER

Änderungshistorie

Vers.	Änderungen	Autor(en)	Fachprüfung durch*	Geprüft am	Freigabe durch	Freigabe am**

*) Fachprüfungen finden nur bei wesentlichen Änderungen des Autors statt.

**) = Datum der in Kraft gesetzten Fassung

Referenzierte Dokumente

Doc-ID	Dokument	Dateiablage und Dateiname
	ISO/IEC 27017	
	BSI Grundschutz	
	NIST Special Publication 800-144 Guidelines on Security and Privacy in Public Cloud Computing	

Es gelten stets die jeweils aktuell in Kraft befindlichen Fassungen.

Inhaltsverzeichnis

#SURVIVEANDPROSPER

1 Ziel und Zweck

Diese Richtlinie orientiert sich an der ISO/IEC 27017 und beschreibt die Beauftragung und den sicheren Umgang von Cloud Computing Diensten.

Die Vorgaben, sind ergänzend zu den Maßnahmen der implementierten Informationssicherheitsmaßnahmen (auf Basis ISO/IEC 27001) zu betrachten.

Sie stellen somit eine Erweiterung der bereits bestehenden Maßnahmen da.

Geltungsbereich und Verantwortungen

Geltungsbereich: XXX

Verantwortungen: siehe die Definition der Rollen und Verantwortlichkeiten dieser Richtlinie

2 Einleitung

Als Cloud-Dienst bezeichnet man das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netzwerk (z.B. Internet). Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Die Spannbreite der im Rahmen von Cloud-Diensten angebotenen Dienstleistungen umfasst das komplette Spektrum der Informationstechnik und beinhaltet unter anderem Infrastruktur (z. B. Rechenleistung, Speicherplatz), Plattformen und Software.

Cloud-Dienste bieten viele Vorteile: Die IT-Dienste können bedarfsgerecht, skalierbar und flexibel genutzt und je nach Funktionsumfang, Nutzungsdauer und Anzahl der Benutzer abgerechnet werden. In der Praxis zeigt sich jedoch häufig, dass sich die Vorteile, die sich Institutionen von der Cloud-Nutzung erwarten, nicht vollständig auswirken. Die Ursache dafür ist meistens, dass wichtige kritische Erfolgsfaktoren nicht ausreichend betrachtet wurden. Daher müssen Cloud-Dienste strategisch geplant sowie Sicherheitsanforderungen, Verantwortungen und Schnittstellen definiert und vereinbart werden. Auch das Bewusstsein und Verständnis für die notwendigerweise geänderten Rollen, sowohl auf Seiten des IT-Betriebs als auch der Benutzer, ist ein wichtiger Erfolgsfaktor.

Zusätzlich sind bei der Einführung von Cloud-Diensten eine Reihe von Governance-Themen wichtig. Beispiele hierfür sind die Vertragsgestaltung, die Umsetzung von Mandantenfähigkeit, die Sicherstellung von Portabilität unterschiedlicher Services, die Abrechnung genutzter Service-Leistungen, das Monitoring der Serviceerbringung, das Sicherheitsvorfallmanagement und zahlreiche Datenschutzaspekte.

3 Hauptteil

3.1 Risiken bei der Nutzung von Cloud-Diensten

Bei der Nutzung von Cloud-Diensten, abgesehen von dem Betrieb einer Private Cloud On-Premise, müssen zusätzliche Risiken betrachtet werden, welche hier stärker zum Tragen kommen als bei einem On-Premise-betrieb.

Daher sind die im Kapitel 5 beschrieben Bedrohungen, im Rahmen des Risiko-management, zu bewerten und geeignete Maßnahmen abzuleiten.

3.2 Erstellung einer Cloud-Nutzungs-Strategie

Für jeden Cloud-Dienst muss eine Cloud-Nutzungs-Strategie erstellt werden. Darin werden die Ziele, Chancen und Risiken definiert, die mit der Cloud-Nutzung verbunden sind. Zudem müssen die rechtlichen und organisatorischen Rahmenbedingungen sowie die technischen Anforderungen untersucht werden, die sich aus der Nutzung des Cloud-Dienstes ergeben. Die Ergebnisse dieser Untersuchung müssen dokumentiert werden.

Es muss festgelegt werden, welche Dienste in welchem Bereitstellungsmodell zukünftig von einem Cloud-Diensteanbieter bezogen werden sollen. Zudem muss sichergestellt werden, dass bereits in der Planungsphase zur Cloud-Nutzung alle grundlegenden technischen und organisatorischen Sicherheitsaspekte ausreichend berücksichtigt werden.

Für den geplanten Cloud-Dienst sollte eine grobe individuelle Sicherheitsanalyse durchgeführt werden. Diese sollte wiederholt werden, wenn sich technische und organisatorische Rahmenbedingungen wesentlich verändern. Für größere Cloud-Projekte muss zudem eine Roadmap erarbeitet werden, die festlegt, wann und wie ein Cloud-Dienst eingeführt wird.

Der Informationssicherheitsbeauftragte und der Datenschutzbeauftragte sind bei der Erstellung der Cloud-Nutzungs-Strategie einzubeziehen.