NEGZ STANDPUNKT

NR. 4 – SICHERHEITSANFORDERUNGEN UND -NACHWEISE BEI CLOUD-DIENSTEN

Stefanie Köhl

NEGZ
Nationales E-Government Kompetenzzentrum e. V.

Die Cloud ist im Einsatz – gesteuert oder ungesteuert – ganz einfach, weil es funktioniert. Diese Entwicklung gilt es, auch vor dem Hintergrund der erhöhten Sicherheitsanforderungen, zukünftig besser zu steuern. Eine der größten Herausforderungen ist die sichere und datenschutzrechtlich konforme Verarbeitung personenbezogener Daten.

Stefanie Köhl, SHI Stein-Hardenberg Institut GmbH

SICHERHEITSANFORDERUNGEN UND -NACHWEISE BEI CLOUD-DIENSTEN — GRUNDLAGEN FÜR ÖFFENTLICHE AUFTRAGGEBER*

Cloud-Systeme bieten eine ressourcensparende Form der IT-Bereitstellung im öffentlichen Sektor, erfordern aber auch eine neuartige IT-Steuerung und erhöhen ggf. die Anforderungen an Sicherheit, weil eine neuartige Komplexität und Verantwortungsketten entstehen. Eine der größten Herausforderungen ist die sichere und datenschutzrechtlich konforme Verarbeitung von personenbezogenen Daten. Nicht-Experten im Bereich IT- und Cloud-Sicherheit müssen in die Lage zu versetzt werden, Anforderungen an eine Cloud-Lösung zu beschreiben, diese zu überprüfen und somit eine fundierte Entscheidung für oder gegen eine bestimmte Cloud-Lösung zu treffen. Diese Auftraggeberkompetenz ist nicht nur für die Auftragsvergabe, sondern auch für die spätere Steuerung des Dienstleisters notwendig und auch vor dem Hintergrund der weiteren technischen Entwicklung dringend erforderlich, um die Abhängigkeit von IT-Anbietern und -Beratern von vornherein zu verringern. Nur so kann die dringend erforderliche Konsolidierung, insbesondere der kommunalen IT, erreicht werden.

* Basierend auf der NEGZ-Kurzstudie „Sicherheitsanforderungen und -nachweise bei Cloud-Diensten – Grundlagen für öffentliche Auftraggeber“. Studienpartner:

SHI STEIN HARDENBERG INSTITUT

6 SCHLAGLICHTER

1. Die Landschaft der existierenden **Standards zu IT-Sicherheit und Datenschutz** bei Cloud-Diensten ist **komplex**. Eine anerkannte Basis-Linie für Sicherheit im Cloud Computing existiert noch nicht. Die vom BSI formulierten **Mindestanforderungen** sind allerdings für eine Leistungs- und Anforderungsbeschreibung **zu abstrakt**.

2. **Kriterienkataloge** können dazu dienen, die **Anforderungen an IT-Sicherheit** und Datenschutz zu **definieren**, da sie die Mindestanforderungen des BSI operationalisieren.

3. Sollten **mehrere Kriterienkataloge** herangezogen werden, sind die einzelnen **Kriterien** voneinander **abzugrenzen bzw. zu matchen**. Denn die meisten Kataloge decken zum größten Teil identische Aspekte ab, sind aber unter Umständen anders formuliert.

4. **Angebote** von Cloud-Anbietern sind zu **überprüfen**, ob die definierten **Anforderungen**, insbesondere bzgl. der Sicherheit, **erfüllt werden**. Auf **Zertifikate** kann man sich i.d.R. **verlassen**, weil diese von akkreditierten Dritten ausgestellt werden. Dennoch wird öffentlichen Verwaltungen **dringend geraten**, auch den **Prüfbericht lesen**, um sich umfassend zu informieren.

5. Die zunehmend an Bedeutung gewinnenden **Selbsterklärungen** auf Basis von anerkannten Verhaltenskodizes sollten **kein Misstrauen** wecken. Sie bilden die **Einstiegsstufe** des Nachweises, den man häufig bei kleineren Anbietern findet, da Zertifizierungen durch Dritte teuer und aufwändig sind.

6. Um den Aufbau einer **Auftraggeberkompetenz** zu unterstützen, sollten die zahlreichen **Anforderungen konsolidiert** und **anwendergerecht operationalisiert** werden. Auf diesem Weg werden öffentliche Verwaltungen besser als bisher in die Lage versetzt, die **Prüfung der Sicherheitsanforderungen** möglichst **selbstständig** vorzunehmen.

FOLGENDE TABELLE STELLT DIE WESENTLICHEN INFORMATIONEN DER IN DER KURZSTUDIE BESCHRIEBENEN STANDARDS BZW. VERHALTENSREGELN ZUSAMMENFASSEND DAR.

Standard	Akteur	Nachweisart	„Prüfstelle“	Laufzeit/Gültigkeit
ISO 27001	Internationale Normungsorganisationen	Zertifikat	Zertifizierte Prüfstelle	3 Jahre, jedoch jährliches Überwachungsaudit
C5	BSI	Testat	Wirtschaftsprüfer	2 Jahre
Trusted Cloud	Kompetenz-netzwerk Trusted Cloud e.V.	Label und öffentliche Anbieterliste	Trusted-Cloud-Beirat	
CCM	Cloud Security Alliance	• Selbsteinschätzung mit öffentlicher Listung • Testat • Zertifikat	• selbst • Wirtschaftsprüfer • Zertifizierte Prüfstelle	s.o., bzw. entsprechend der Prüfsysteme
EuroCloud	EuroCloud	Zertifikat	Von EuroCloud akkreditierte Partner	2 Jahre
TCDP/Auditor	Bundesstiftung Datenschutz	Zertifikat	Zertifizierungsstelle	n.a.
DSGVO Verhaltenskodex	Cloud Security Alliance	• Selbsteinschätzung • Zertifikat	• selbst • Zertifizierungsstelle	n.a.

Die Cloud bietet durch Bündelungseffekte standardisierter Dienstleistungen erhebliche Potenziale für Effizienzsteigerungen und kann so eine verstärkte IT-Konsolidierung unterstützen. Obwohl die Bedenken gegenüber Cloud, insbesondere bezüglich Sicherheit, Datenschutz und den gesetzlichen Anforderungen, immer noch vorhanden sind, gibt es in der Cloud de facto höhere Sicherheit, als im eigenen Rechenzentrum. Diese Unsicherheit ist eher dem Mangel an IT-Sicherheitsfachkräften und den unzureichenden Kenntnissen geschuldet.

Darüber hinaus stellen sich mit der Cloud aber noch weitere Herausforderungen, um die häufig vorkommenden Multi-Cloud-Lösungen erfolgreich zu verwalten und interoperabel zu gestalten. Daher ist die Entscheidung für die Cloud immer mit einer Risikoabschätzung anzugehen

Gerade für den Prozess der öffentlichen Beschaffung ist eine Fundierung durch eine Cloud-Strategie zu empfehlen, da sich so nicht nur die Chance auf mehr Sicherheit erhöht, sondern auch die Prozesse für die Konformität mit der DSGVO neu abgebildet werden können.

Linda Strick, Direktorin des European Headquarter der Cloud Security Alliance

VERANSTALTUNGEN NEGZ

NEGZ Herbsttagung 2019

22. Oktober 2019, Berlin

Der inhaltliche Schwerpunkt liegt auf dem Thema „Digitale Souveränität“ mit all seinen Perspektiven (Bürger, Unternehmen, Verwaltung) und Facetten.

Zum Auftakt wird ein Slam „Souveränität – Mitglieder nehmen Stellung” die Meinungsvielfalt und die unterschiedlichen Perspektiven der im NEGZ engagierten Mitglieder präsentieren.

Die unterschiedlichen Perspektiven werden in Vorträgen vertieft und zum Abschluss in einer Podiumsdiskussion kontrovers diskutiert. Diskutanten sind Prof. Dr. Jörg Becker (ERCIS, WWU Münster), Dr. Johann Bizer (Dataport), Franz-Reinhard Habbel, Roland Jabkowski (Co-CIO Hessen), Andreas Kleinknecht (Microsoft).

Hierzu laden wir Sie herzlich ein.

Anmeldung | Programm

N3GZ-Workshop „Kooperationen in der Verwaltungsdigitalisierung“

29. Oktober 2019, Lübeck

Die Digitalisierung der öffentlichen Verwaltung ist ein Teamsport: Ihre Umsetzung erfordert oft die Zusammenarbeit von Akteuren aus Verwaltung, Wirtschaft und Zivilgesellschaft.

Angesprochen sind Nachwuchskräfte, die sich mit Kooperationen in der Verwaltungsdigitalisierung beschäftigen. Der Workshop findet mit freundlicher Unterstützung der Mach AG am Vortag der „Innovatives Management“-Konferenz statt.

Mehr Infos und Anmeldung

IMPRESSUM

Basierend auf der NEGZ-Kurzstudie „Sicherheitsanforderungen und -nachweise bei Cloud-Diensten — Grundlagen für öffentliche Auftraggeber“, Autorinnen: Stefanie Köhl, Heidrun Müller

Aus der Reihe „Berichte des NEGZ“, Nr. 7, ISSN: 2626-6032,
DOI: 10.30418/2626-6032.2019.07

Für einen modernen Staat

Das Nationale E-Government Kompetenzzentrum vernetzt Expertinnen und Experten aus Politik, Verwaltung, Wissenschaft und Wirtschaft. Das NEGZ versteht sich als die zentrale, unabhängige Plattform für Staatsmodernisierung und Verwaltungstransformation in Deutschland.

PDF-DOWNLOAD KURZSTUDIE →

PROJEKTE & PUBLIKATIONEN DES NEGZ →

Nationales E-Government Kompetenzzentrum e. V.

Pressehaus / 4102
Schiffbauerdamm 40
10117 Berlin

+49 (0)30 80494747
info@negz.org
negz.org

Gestalterische Umsetzung
made in – Design und Strategieberatung
www.madein.io