essentials

essentials liefern aktuelles Wissen in konzentrierter Form. Die Essenz dessen, worauf es als „State-of-the-Art“ in der gegenwärtigen Fachdiskussion oder in der Praxis ankommt. *essentials* informieren schnell, unkompliziert und verständlich

- als Einführung in ein aktuelles Thema aus Ihrem Fachgebiet
- als Einstieg in ein für Sie noch unbekanntes Themenfeld
- als Einblick, um zum Thema mitreden zu können

Die Bücher in elektronischer und gedruckter Form bringen das Expertenwissen von Springer-Fachautoren kompakt zur Darstellung. Sie sind besonders für die Nutzung als eBook auf Tablet-PCs, eBook-Readern und Smartphones geeignet. *essentials:* Wissensbausteine aus den Wirtschafts-, Sozial- und Geisteswissenschaften, aus Technik und Naturwissenschaften sowie aus Medizin, Psychologie und Gesundheitsberufen. Von renommierten Autoren aller Springer-Verlagsmarken.

Weitere Bände in der Reihe http://www.springer.com/series/13088

Michael Adelmeyer · Christopher Petrick
Frank Teuteberg

IT-Risikomanagement von Cloud-Services in Kritischen Infrastrukturen

HMD Best Paper Award 2017

Mit einem Geleitwort von
Prof. Dr. Matthias Knoll

Springer Vieweg

Michael Adelmeyer
Osnabrück, Deutschland

Frank Teuteberg
Osnabrück, Deutschland

Christopher Petrick
Osnabrück, Deutschland

Das essential ist eine überarbeitete und erweiterte Version des Artikels: Adelmeyer, Petrick, Teuteberg (2017). IT-Risikomanagement von Cloud-Dienstleistungen im Kontext des IT-Sicherheitsgesetzes. HMD – Praxis der Wirtschaftsinformatik 54 (1), S. 111–123 sowie Adelmeyer, Petrick, Teuteberg (2018) Cloud-Services in Kritischen Infrastrukturen – Anforderungen und IT-Risikomanagement, in: Edition HMD, Cloud Computing – Die Infrastruktur der Digitalisierung, Reinheimer, S. (Hrsg.), S. 199–214.

ISSN 2197-6708 ISSN 2197-6716 (electronic)
essentials
ISBN 978-3-658-22741-8 ISBN 978-3-658-22742-5 (eBook)
https://doi.org/10.1007/978-3-658-22742-5

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Springer Vieweg

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier

Springer Vieweg ist ein Imprint der eingetragenen Gesellschaft Springer Fachmedien Wiesbaden GmbH und ist ein Teil von Springer Nature
Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

Was Sie in diesem *essential* finden können

- Eine Einführung in das Cloud Computing und das IT-Sicherheitsgesetz
- Einen Anforderungskatalog für Cloud-Services zur Sicherstellung der Compliance mit dem IT-Sicherheitsgesetz
- Grundlagen des Risikomanagements von Cloud-Services vor dem Hintergrund des IT-Sicherheitsgesetzes
- Bewertung von Szenarien und Rollen von Cloud-Services im Kontext Kritischer Infrastrukturen
- Handlungsempfehlungen für Cloud-Nutzer und Cloud-Dienstleister

Geleitwort

Der prämierte Beitrag

Die Digitalisierung der Wirtschaft und des Privaten schreitet seit einigen Jahren stetig voran und ist daher vielleicht nicht immer und überall gleich stark erkennbar. Doch die Folgen dieser Digitalisierung sind weitreichend. Selbst in Branchen und an Orten, an denen man es weniger vermuten würde, entstanden und entstehen neue Geschäftsmodelle oder gar neue Unternehmen. Kundenbindung wird – etwa durch Dienstleistungen großer E-Commerce-Unternehmen wie beispielsweise die Abo-Modelle für E-Books, Musik und Filme, oder durch neuartige Angebote wie beispielsweise eine vorausschauende Wartung im Maschinen- und Anlagensektor – neu definiert.

In gleichem Maß ändern sich unsere Nutzungsgewohnheiten digitaler Technologien und ihrer „Produkte". An der einen Stelle schneller, etwa bei Smartphones oder den sogenannten Wearables wie Fitness-Tracker, vielleicht auch, weil der Druck des sozialen Umfeldes uns dazu zu zwingen scheint. An anderer Stelle langsamer, etwa bei Smart Home, das aufgrund (zu) vieler konkurrierender Standards und verschiedener technischer Implikationen nur zögerlich in Privathaushalte Einzug hält.

Doch der Trend zu immer mehr IT, zu einer internetbasierten allumfassenden Vernetzung von Menschen und Maschinen und damit zu einer nicht nur gefühlt unaufhaltsam, gar exponentiell weiterwachsenden Abhängigkeit von der IT ist unumkehrbar. Das Interessante und Beunruhigende zugleich: Sektoren, die bislang eher weniger betroffen waren, sind längst mit dabei.

Einige Beispiele: Die Energiewende führt zu einer Dezentralisierung der Stromnetze und damit zu neuen Regelungs- und Lastverteilmechanismen, die nur mit IT-Unterstützung realisiert werden können. Aus dem Bahn- und Flugverkehr ist IT ebenfalls nicht mehr wegzudenken. Der Straßenverkehr in großen

Städten, die Wasserversorgung und andere Infrastruktur-Dienstleistungen werden mittlerweile durch spezielle Anwendungen zentral gesteuert. In Krankenhäusern und Arztpraxen fließen hochsensible Patienten- und Diagnosedaten durch das Netzwerk, sind praktisch alle Geräte aus den medizinischen Bereichen miteinander und wie selbstverständlich auch mit den Systemen der Verwaltung vernetzt. Selbst in der Ernährungsbranche, etwa in der Produktion von Nahrungsmitteln, ist ein stark zunehmender IT-Einsatz zu beobachten.

Diese Beispiele haben eine Gemeinsamkeit: Sie sind wesentlicher Bestandteil unseres Gemeinwesens, erfüllen eine öffentliche Aufgabe und tragen zu Sicherheit und Wohlstand in unserer Gesellschaft bei.

Der IT-Einsatz verspricht hierbei eine interessante neue Zukunft, in der die Möglichkeiten für Unternehmen und Bürger vielfältiger sein werden. Doch ist das wirklich so? Allzu gerne werden bei solchen Szenarien mögliche Risiken in den Hintergrund gedrängt. Denn Risiken sind „Spielverderber".

Aus diesem Grund hat die Bundesregierung für acht zentrale Sektoren (Energie, IT und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanzen und Versicherungen) in enger Zusammenarbeit mit Behörden, insbesondere dem Bundesamt für Sicherheit in der Informationstechnik, den Begriff „Kritische Infrastruktur" definiert. Für Aufbau und Betrieb solcher Kritischen Infrastrukturen gelten besondere Regeln, die der deutsche Gesetzgeber mit dem IT-Sicherheitsgesetz (IT-SiG) im Sinne einer Stärkung der IT-Sicherheit in diesem Bereich festgelegt hat. Als Artikelgesetz erweitert es bestehende Gesetze wie etwa das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG), das Atomgesetz (AtG), das Energiewirtschaftsgesetz (EnWG), das Telekommunikationsgesetz (TKG) und weitere Gesetze. Zudem beziehen sich zahlreiche nachgeordnete Vorgaben auf das IT-Sicherheitsgesetz.

Parallel zu diesen Entwicklungen hat sich in den letzten Jahren der Einsatz von Cloud-Technologien und -Lösungen außerhalb Kritischer Infrastrukturen als „State-of-the-Art" oder „Best Practice" etabliert. Anfängliche Probleme wurden gelöst, viele Unternehmen aus allen Branchen vertrauen auch für teilweise unternehmenskritische Anwendungen auf die flexible und leicht skalierbare und häufig auch kostenseitig attraktive Möglichkeit, IT-Services aus der Cloud zu nutzen.

Als „Sonderform" des Outsourcings erbt Cloud Computing die damit verbundenen typischen Risiken. Einige neue Risiken kommen hinzu, etwa die deutlich größere Anonymität in der Geschäftsbeziehung und die damit verbundenen Unsicherheiten hinsichtlich der exakten Konfiguration, des genauen Ortes der Verarbeitung oder Speicherung von Daten oder der Beschränkung im Customizing sowie der Einhaltung von fachlichen und technischen Vorgaben und Standards.

Vielfach können diese Risiken akzeptiert werden, denn die Folgen bei Risikoeintritt beschränken sich auf das betroffene Unternehmen, dessen Angebote und dessen Kunden.

Anders sieht es in Unternehmen aus, die zur Kritischen Infrastruktur gehören. Der Einsatz von Cloud-Services im Umfeld Kritischer Infrastrukturen (KRITIS) stellt an alle Beteiligten besondere Anforderungen. Denn die Auswirkungen von Risiken können hier weitaus dramatischer sein, bis hin zu gesundheitlichen Beeinträchtigungen oder gar lebensbedrohlichen Situationen. Hier sollte also nicht „eben mal" ein Cloud-Service hinzugebucht und unreflektiert genutzt werden.

Das vorliegende *essential* greift diese Fragestellungen umfassend auf. Es geht auf einen Beitrag aus der Schwerpunktausgabe 313 der Zeitschrift HMD – Praxis der Wirtschaftsinformatik zum Thema „IT-Risikomanagement" sowie auf einen Beitrag aus der Fachbuchreihe Edition HMD zum Thema „Cloud Computing" zurück. Der Originalbeitrag aus der HMD 313 zählte zu den drei Gewinnern des HMD Award 2017 und erschien nicht nur aus diesem Grund in besonderer Weise für ein *essential* geeignet.

Der Beitrag enthält neben einer leicht verständlichen theoretischen Einführung des Cloud Computings, des IT-Sicherheitsgesetzes und des IT-Risikomanagements im Cloud-Kontext einen strukturiert aufgebauten Anforderungskatalog für Cloud-Services unter dem Gesichtspunkt der Sicherstellung der Compliance mit dem IT-Sicherheitsgesetz.

Den Hauptteil des Beitrags bilden eine Bewertung von Szenarien und der Position und Bedeutung von Cloud-Services im Kontext Kritischer Infrastrukturen sowie konkrete Handlungsempfehlungen für Cloud-Nutzer und Cloud-Dienstleister, vielfach als direkt verwertbare Tipps und Hinweise in Checklistenform. Er hilft damit einerseits den Unternehmen im KRITIS-Sektor bei der Entscheidung für oder gegen solche Lösungen und im Alltag mit ihnen, andererseits enthält er wertvolle Hinweise für Betreiber von Cloud-Lösungen für die KRITIS-Sektoren.

Die HMD – Praxis der Wirtschaftsinformatik und der HMD Best Paper Award

Alle HMD-Beiträge basieren auf einem Transfer wissenschaftlicher Erkenntnisse in die Praxis der Wirtschaftsinformatik. Umfassendere Themenbereiche werden in HMD-Heften aus verschiedenen Blickwinkeln betrachtet, sodass in jedem Heft sowohl Wissenschaftler als auch Praktiker zu einem aktuellen Schwerpunktthema zu Wort kommen. Den verschiedenen Facetten eines Schwerpunktthemas geht ein Grundlagenbeitrag zum State of the Art des Themenbereichs voraus. Damit liefert die HMD IT-Fach- und Führungskräften Lösungsideen für ihre Probleme, zeigt ihnen Umsetzungsmöglichkeiten auf und informiert sie über Neues in der

Wirtschaftsinformatik. Studierende und Lehrende der Wirtschaftsinformatik erfahren zudem, welche Themen in der Praxis ihres Faches Herausforderungen darstellen und aktuell diskutiert werden.

Wir wollen unseren Lesern und auch solchen, die HMD noch nicht kennen, mit dem „HMD Best Paper Award“ eine kleine Sammlung an Beiträgen an die Hand geben, die wir für besonders lesenswert halten, und den Autoren, denen wir diese Beiträge zu verdanken haben, damit zugleich unsere Anerkennung zeigen. Mit dem „HMD Best Paper Award“ werden alljährlich die drei besten Beiträge eines Jahrgangs der Zeitschrift „HMD – Praxis der Wirtschaftsinformatik“ gewürdigt. Die Auswahl der Beiträge erfolgt durch das HMD-Herausgebergremium und orientiert sich an folgenden Kriterien:

- Zielgruppenadressierung
- Handlungsorientierung und Nachhaltigkeit
- Originalität und Neuigkeitsgehalt
- Erkennbarer Beitrag zum Erkenntnisfortschritt
- Nachvollziehbarkeit und Überzeugungskraft
- Sprachliche Lesbarkeit und Lebendigkeit

Alle drei prämierten Beiträge haben sich in mehreren Kriterien von den anderen Beiträgen abgesetzt und verdienen daher besondere Aufmerksamkeit. Neben dem Beitrag von Michael Adelmeyer, Christopher Petrick und Frank Teuteberg wurden ausgezeichnet:

- B. Spottke: Was Unternehmen von der Videospielindustrie für die Gestaltung der Digital Customer Experience lernen können. HMD – Praxis der Wirtschaftsinformatik 54 (2017), 317, S. 727–740.
- S. Rohmann, M. Schumann: Best Practices für die Mitarbeiter-Partizipation in der Produktentwicklung. HMD – Praxis der Wirtschaftsinformatik 54 (2017), 316, S. 575–590.

Die HMD ist vor mehr als 50 Jahren erstmals erschienen: Im Oktober 1964 wurde das Grundwerk der ursprünglichen Loseblattsammlung unter dem Namen „Handbuch der maschinellen Datenverarbeitung“ ausgeliefert. Seit 1998 lautet der Titel der Zeitschrift unter Beibehaltung des bekannten HMD-Logos „Praxis der Wirtschaftsinformatik“, seit Januar 2014 erscheint sie bei Springer Vieweg. Verlag und HMD-Herausgeber haben sich zum Ziel gesetzt, die Qualität von HMD-Heften und -Beiträgen stetig weiter zu verbessern. Jeder Beitrag wird dazu nach Einreichung doppelt begutachtet: Vom zuständigen HMD- oder

Gastherausgeber (Herausgebergutachten) und von mindestens einem weiteren Experten, der anonym begutachtet (Blindgutachten). Nach Überarbeitung durch die Beitragsautoren prüft der betreuende Herausgeber die Einhaltung der Gutachtervorgaben und entscheidet auf dieser Basis über Annahme oder Ablehnung.

Es ist mir als betreuendem Herausgeber der Heftes 313 der Zeitschrift HMD – Praxis der Wirtschaftsinformatik eine große Freude, in diesen nunmehr stark erweiterten und nochmals inhaltlich überarbeiteten Beitrag einführen zu dürfen. Mein herzlicher Dank gilt dem Autorenteam, das sich sofort für eine Ausarbeitung in diesem Rahmen begeistern konnte. Ich wünsche Ihnen eine spannende Lektüre, aus der Sie viel Wissen mitnehmen können.

Darmstadt Matthias Knoll

Literatur

Adelmeyer M, Petrick C, Teuteberg F (2017) IT-Risikomanagement von Cloud-Dienstleistungen im Kontext des IT-Sicherheitsgesetzes. HMD – Praxis der Wirtschaftsinformatik 54(1), 313, S 111–123

Adelmeyer, Petrick, Teuteberg (2018) Cloud-Services in Kritischen Infrastrukturen – Anforderungen und IT-Risikomanagement, in: Edition HMD, Cloud Computing – Die Infrastruktur der Digitalisierung, Reinheimer, S. (Hrsg.), S. 199–214.

Inhaltsverzeichnis