UMSTIEG IN DIE CLOUD... *mit Sicherheit*

TEIL 3 VON 3

AUS DEM INHALT

9 PROTOKOLLIERUNG UND ÜBERWACHUNG

Letztendlich unterstützen Ereignisprotokolle die Rückverfolgbarkeit von Ereignissen im Falle eines Sicherheitsvorfalls. Dies setzt voraus, dass Ereignisse, die zur Ermittlung der Ursachen notwendig sind, aufgezeichnet und gespeichert werden. Darüber hinaus ist die Protokollierung und Analyse von Aktivitäten gemäß der geltenden Gesetzgebung (z. B. Datenschutz- oder Betriebsverfassungsgesetz) erforderlich, um festzustellen, welches Benutzerkonto Änderungen an IT-Systemen vorgenommen hat.

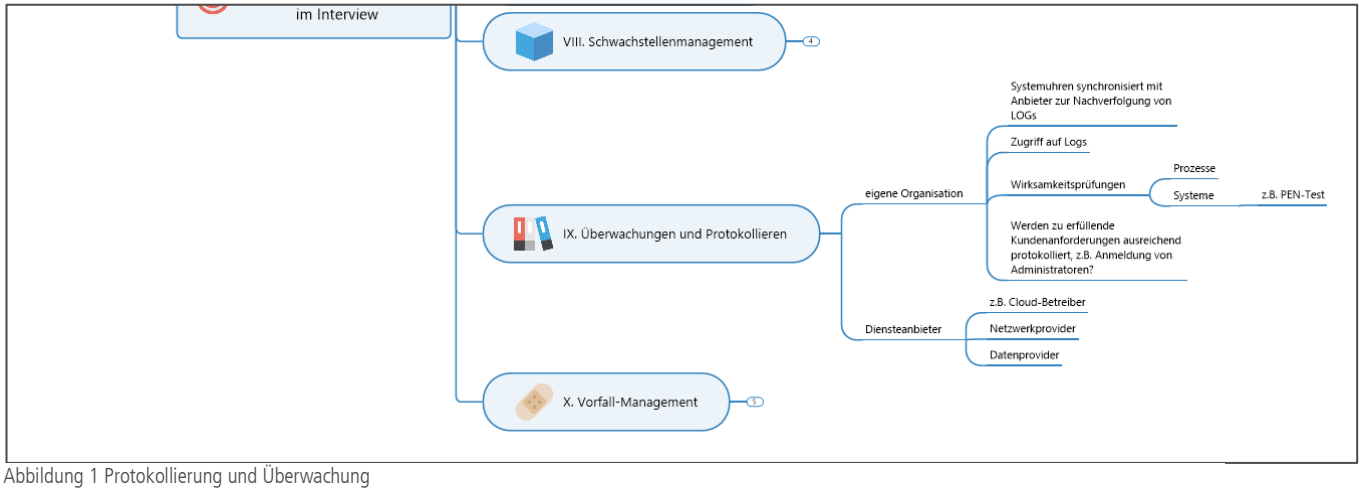

Abbildung 1 Protokollierung und Überwachung

Mögliche Kontrollfragen können hier sein:

- Inwieweit sind organisationsfremde Dienste in die eigene Infrastruktur integriert? Inwieweit lassen sich Kommunikationswege tatsächlich rückverfolgen, z.B. indem die Systemuhren mit der eigenen IT synchronisiert sind?
- Welche Möglichkeiten der Protokollierung bietet der Dienst tatsächlich an (z.B. Protokollierung über Aktivitäten der Benutzerverwaltung), um die eigenen Anforderungen abzudecken?
- Bestehen zusätzliche Anforderungen (z.B. Einhaltung von gesetzlichen Löschfristen personenbezogener Daten) an die Protokollierung seitens Kunden, Behörden oder aus dem Datenschutz und reicht die Protokollierung aus?
- Wer im Unternehmen des Diensteanbieters kann Aktivitäten des eigenen Unternehmens einsehen?
- Erfolgt die Protokollierung im Einklang mit gesetzlichen Bestimmungen (z.B. Überwachung)?
- Werden Protokolle regelmäßig und revisionssicher aufbewahrt?
- Bestehen besondere Aufzeichnungsanforderungen aus Kundenaufträgen, wie beispielsweise Zugriffe aus Kundenaufträgen?

10 VORFALL-MANAGEMENT

Im Zuge ausgelagerter Services können Informationssicherheitsereignisse entstehen, die angemessen gemanaged werden müssen, insbesondere, um möglichen Schaden zu begrenzen und ein wiederholtes Eintreten zu verhindern. Dazu ist es wichtig, mit dem Diensteanbieter eine gemeinsame Verfahrensweise zur Meldung, Erfassung und Bearbeitung von Informationssicherheitsereignissen/-schwachstellen zu definieren und umzusetzen, wie z.B. Verhalten bei Informationssicherheitsereignissen/-schwachstellen, Meldeformular und Meldeweg, bearbeitende Stellen und Feedbackverfahren.

Dabei muss sichergestellt sein, dass Informationssicherheitsereignisse/-schwachstellen bewertet und zur Sicherstellung der Nachweisbarkeit dokumentiert werden. Eine angemessene Reaktion auf Informationssicherheitsereignisse/-schwachstellen ist obligatorisch sowie auch Reglungen und Vorgehensweisen zur Eskalation, Wiederherstellung und Kommunikation an relevante interne und externe Stellen. Auch muss die Vorgehensweise zur Entscheidung, ob ein Cybercrime-Angriff strafrechtlich verfolgt wird, festgelegt sein.

Oft bestehen Anforderungen von Dritten, z.B. vertraglich vereinbarte Meldepflichten, die vertragskonform bedient werden müssen, so dass dieses bei Eintritt nicht mit zusätzlichen Schadenersatzansprüchen geahndet wird.

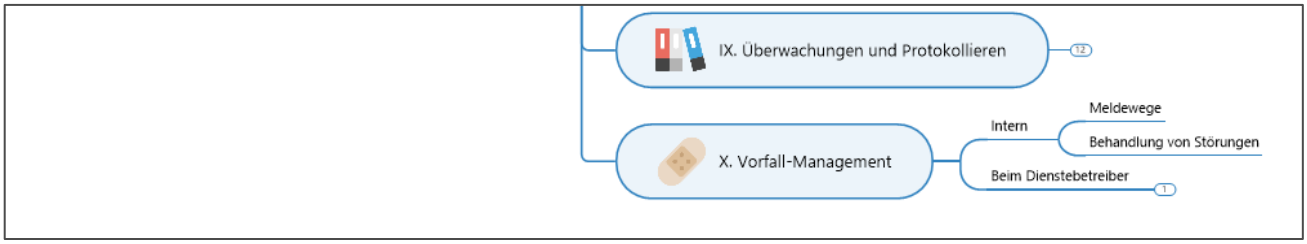

Abbildung 2 Vorfall-Management

Mögliche Kontrollfragen können hier sein:

- Welche Verantwortlichkeiten ergeben sich bei der Meldung von Sicherheitsereignissen?
- Wie erfolgt die Meldung und wie sind die Meldewege?
- Ist eine ausreichende Verfügbarkeit – auch eigenes Personal – gegeben bzw. können Störungen ausreichend schnell an den Diensteanbieter übermittelt werden?
- Reichen die vereinbarten Response-Zeiten und passen die Parameter zu den ermittelten maximal tolerierbaren Ausfallzeiten kritischer Systeme?
- Bestehen ggf. vertraglich vereinbarte Meldepflichten mit eigenen Kunden?

11 ABGRENZUNG UND ABHÄNGIGKEITEN

Wie bereits zuvor erwähnt, überrascht der generelle Ablauf nicht und ähnelt doch sehr dem üblichen Change und der Untersuchung bei allen neuen Systemen im Unternehmen. Entsprechend sind die Aspekte der Informationssicherheit bei der Auswahl von Clouddiensten durchweg vernetzt.

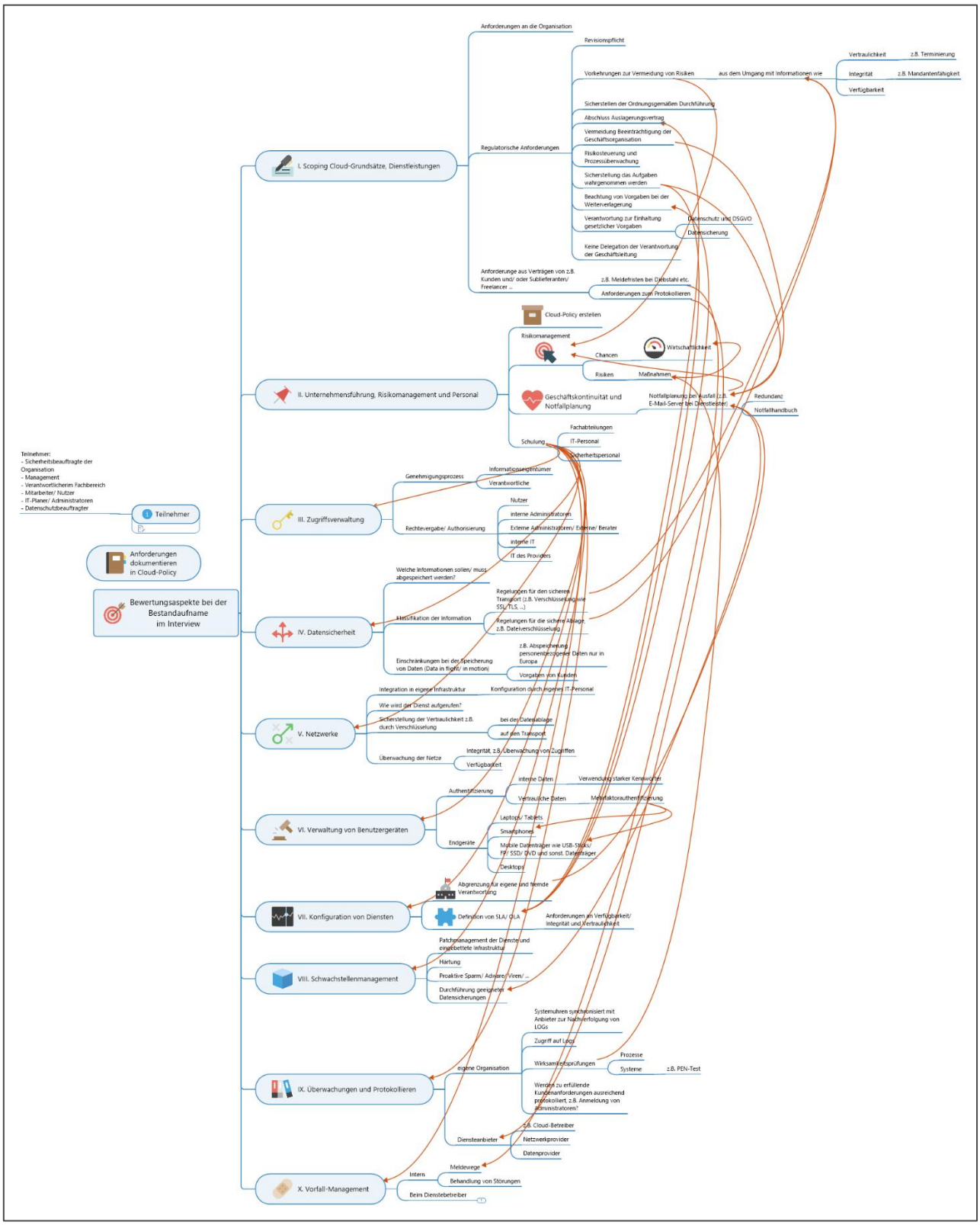

Abbildung 3 Abhängigkeiten und Vernetzung

Der genaue Pfad verbleibt – wie immer – in der eigenen Verantwortung des Unternehmens und ist entsprechend unternehmensspezifisch zu gestallten. Die Beschreibung der vollständigen Vernetzung kann dieser Beitrag daher nicht leisten, bietet jedoch einen ersten sinnvollen Beratungsansatz für den strukturierten Umstieg.

12 FAZIT

Der Wechsel von Diensten und Services in die Cloud und damit der Verschiebung von Verantwortung bietet seitens der Anforderungen an die Informationssicherheit viele Vorteile und neue Möglichkeiten und stellt definitiv eine Verbesserung dar. Im Rahmen eines wirksamen Informationssicherheitsmanagementsystems bleibt es im Vorfeld unabdingbar, sich auch detailliert mit den neuen Services auseinander zu setzen. Dieses sollte strukturiert und mit dem erforderlichen Fachwissen erfolgen. Es müssen die „richtigen" Fragen geklärt werden. Eine Service-Konfiguration kann nicht durch nur durch ein Zertifikat wie ISO27001 oder TISAX® aufgefangen werden.

Um Risiken zu managen ist es unabdingbar, hier zu wissen „was tatsächlich läuft". Es ist im Vorfeld die essenzielle Aufgabe der eigenen Organisation, für ausreichende Schulung und intensive Auseinandersetzung mit verbleibenden Risken zu sorgen. Ein strukturiertes Vorgehen und eine genaue Analyse und Bewertung helfen beim Umstieg. Der Aufwand hierfür entspricht vermutlich dem adäquaten Aufwand bei der Evaluierung neuer interner IT-Systeme und ist nicht zwangsläufig höher. Zusätzliche Dienste fügen sich sehr oft in einen bestehenden Ansatz mit ein, so dass von einem geringeren Folgeaufwand ausgegangen werden kann.

Eines der wichtigsten Themen überhaupt ist auch immer die Frage nach der Verantwortlichkeit. „Shared Responsibilities" ist möglich, es ist jedoch zu klären, wo und wie vertraglich klare Grenzen gezogen sind. Aus gutem Grund legen externe Auditoren gerne den Finger in die Wunde und fordern eindeutige dokumentierte Verantwortungen.

Die Untersuchung der Möglichkeiten für einen Umstieg lohnt sich in vielen Fällen, da sich neben den beschriebenen wirtschaftlichen Vorteilen auch deutliche Verbesserungen der eigenen Informationssicherheit erzielen lassen. Die ergeben sich allerdings nicht - wie oft fälschlich angenommen - von allein, so dass hier die eigene Organisation handeln muss. Der Umstieg gelingt jedoch oft schnell mit vielen Vorteilen - wenn er strukturiert erfolgt.

In eigener Sache: Auf Basis des vorliegenden Artikels wurde in der Podcast-Serie „Isitalk" (HTTPS://ISITALK.PODIGEE.IO/7-CLOUD2 oder auch zu finden bei allen einschlägigen Podcast-Anbietern wie Spotify, Apple-Musik u.a.) ein inhaltlich angelehnter Beitrag anhand eines konkreten Fallbeispiels zum Umstieg der eigenen Microsoft-Umgebung in die „Outlook 365" Umgebung diskutiert, der diesen Beitrag um ein konkretes Fallbeispiel ergänzt.

Der Autor Bernd Schart ist seit 2009 Mitarbeiter der OS und beschäftigt sich im Fachgebiet Security & Audit seit 2011 als Auditor mit dem Thema Informationssicherheit in der Automobilindustrie. Bernd Schart betreibt seit 2020 einen eigenen, freien und unabhängigen Podcast (WWW.ISITALK.DE) zu Themen der Informationssicherheit, speziell auch den Anforderungen des VDA ISA im Rahmen von TISAX® Assessments.