DataNavigator

www.datanavigator.de | ISSN 2702-1904

Der Informationsverbund – Daten (nur) für die Aufsicht?

Kristian Buric

#12 | Juli 2022

EUROGROUP CONSULTING

Im Juni 2021 kam es zu einem folgenschweren Cyberangriff auf die IT der Volks- und Raiffeisenbanken. Kunden von 820 VR-Banken hatten temporär keinen Zugriff mehr auf das Online-Banking.[1]

Bei Cyberangriffen wie diesem kommt es auf Reaktionsgeschwindigkeit an. Sind die Verantwortlichkeiten klar geregelt, um schnell einen Krisenstab zusammenzustellen? Ist die eigene Anwendungs- und Infrastrukturlandschaft transparent genug, um den Angriff schnell zu lokalisieren und Gegenmaßnahmen einzuleiten? Diesen und ähnlichen Fragen rund um den eigenen „Informationsverbund" müssen sich Führungskräfte in der Finanzdienstleistungsbranche stellen – nicht zuletzt, weil es die Aufsichtsbehörden fordern.

Der Informationsverbund und die aufsichtsrechtlichen Anforderungen an Finanzdienstleister

Der Informationsverbund findet Erwähnung in den aufsichtsrechtlichen Anforderungen an die IT von Banken (sog. BAIT), von Versicherungen (VAIT) und von Kapitalverwaltungsgesellschaften (KAIT). Dabei konkretisieren diese Anforderungen bereits seit einigen Jahren geltende Gesetze (z.B. KWG, MaRisk für Banken) zum ordnungsgemäßen Geschäftsbetrieb von Finanzdienstleistern. Die Einhaltung der BAIT/VAIT/KAIT und damit auch die Abbildung des Informationsverbunds werden zunehmend von den Aufsichtsbehörden in Sonderprüfungen untersucht. Was aber ist ein Informationsverbund?

Der Informationsverbund umschreibt die schützenswerten Informationen sowie die Gesamtheit der Mittel zur Verarbeitung dieser schützenswerten Informationen im Unternehmen. Wie Abbildung 1 zeigt, wird dabei zwischen folgenden Elementen („IV-Elementen") unterschieden:

- Informationscluster bzw. Datenkategorien sind die im Unternehmen verarbeiteten bzw. gespeicherten, schützenswerten Informationen. Diese sind in Cluster bzw. Kategorien zusammenzufassen und hinsichtlich der Schutzbedarfe „Vertraulichkeit" und „Integrität/Authentizität" einzuwerten. So sind z.B. Informationen der

[1] Vgl. https://www.handelsblatt.com/finanzen/banken-versicherungen/banken/it-dienstleister-sabotageangriff-legt-onlinebanking-bei-mehr-als-820-banken-lahm/27256270.html

Kategorie „öffentliche Verzeichnisse“ wie z.B. Handelsregisterdaten mit geringen Anforderungen an die Vertraulichkeit verbunden im Vergleich zu personenbezogenen Daten, die i.d.R. einen hohen Schutzbedarf haben.

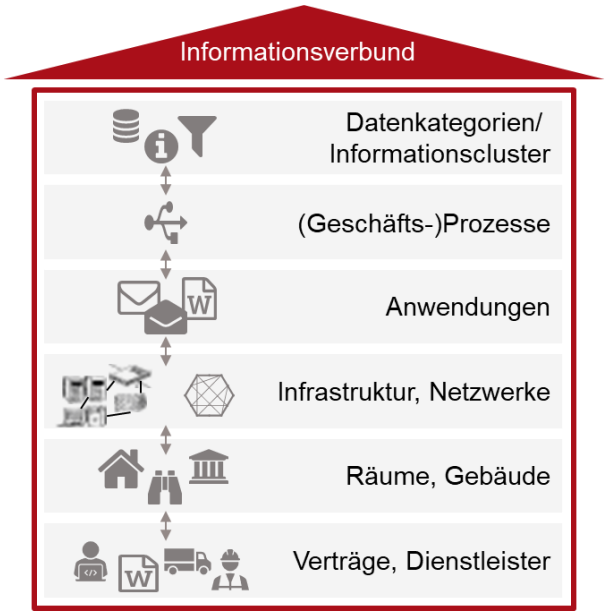

Abbildung 1 - Die Elemente des Informationsverbunds

- Das IV-Element Prozesse umfasst alle Geschäftsprozesse sowie Unterstützungsprozesse (z.B. IT-Prozesse). Für eine aufsichtsrechtlich konforme Abbildung des Informationsverbunds ist häufig ein mittlerer Detaillierungsgrad der Prozesse bzw. Prozessbeschreibungen ausreichend.
- Zum IV-Element Anwendungen gehört jegliche Software zur Umsetzung bzw. Unterstützung der Prozesse bzw. Tätigkeiten im Unternehmen. I.d.R. ist hier die Kernbankanwendung genauso zu erfassen wie ein im Fachbereich verwendetes Excel-Tool.
- Das IV-Element IT-Infrastruktur beschreibt alle informationsverarbeitenden Geräte und Netzwerke im Unternehmen. Hierfür werden die Infrastrukturkomponenten i.d.R. nach Typen zusammengefasst. So kann z.B. ein Gerätetyp „Thin Client“ einen geringen Schutzbedarf aufweisen, wenn auf diesen Geräten keine Daten persistent gespeichert werden.
- Auch Gebäude bzw. Räume, also die physischen Lokationen eines Unternehmens, sind zur Abbildung des Informationsverbunds zu definieren. Damit soll ersichtlich werden, an welchen Orten höhere Schutzvorkehrungen zu treffen sind, wie z.B. für Serverräume oder Tresorräume.
- Um die Abbildung des Informationsverbunds zu vervollständigen, sind auch alle relevanten Lieferanten- und Dienstleister-Verträge und Vertragspartner des Unternehmens abzubilden - insbesondere solche, die einen Auslagerungssachverhalt darstellen.

Um den Informationsverbund zu schützen, sind grundsätzlich die Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität zu wahren. Daher sind für alle Elemente des

Informationsverbunds entsprechende Schutzbedarfe festzulegen. Der Aufwand dafür ist je nach IV-Element und Menge der Unterkategorien unterschiedlich groß. Ergebnis der Schutzbedarfsfeststellung ist eine Einteilung in Kategorien wie niedrig/mittel/hoch und eine Begründung für diese Einteilung.

Schutzbedarfe werden aufgrund der Zusammenhänge zwischen den IV-Elementen vererbt, d.h. von einem auf das andere zusammenhängende IV-Element übertragen. Zum Beispiel erhält ein Prozess „Kontoeröffnung", der personenbezogene Daten wie Kontodaten verarbeitet, automatisch einen hohen Schutzbedarf hinsichtlich des Schutzziels Vertraulichkeit vererbt, da die dazugehörige Datenkategorie einen hohen Schutzbedarf vorsieht. Dies reduziert einerseits den Aufwand der Schutzbedarfsfeststellung, andererseits erhöht es damit aber auch die Komplexität der Abbildung des Informationsverbunds. Häufig ist deswegen der Einsatz von spezieller Compliance-Software notwendig, um die unterschiedlichen Zusammenhänge des Informationsverbunds abbilden und strukturiert wieder abrufen zu können.

Governance des Informationsverbunds

Zur Dokumentation des Informationsverbunds ist es notwendig aufbau- und ablauforganisatorische Vorkehrungen zu treffen. Die initiale Abbildung des Informationsverbunds kann projekthaft erfolgen. Spätestens für die laufende Pflege und Aktualisierung sind dedizierte Verantwortliche zu benennen. So ist ein „Informationsverbund-Koordinator" zu definieren, der für die übergreifende Qualitätssicherung und laufende Pflege verantwortlich ist. Daneben sollten für die einzelnen IV-Elemente (wie z.B. Anwendungen) entsprechende „IV-Element-Verantwortliche" benannt werden, die für die Qualitätssicherung der Daten auf Detailebene verantwortlich sind. Wir empfehlen, dass sich der „IV-Koordinator" mit den „IV-Element-Verantwortlichen" in regelmäßigen Abständen über Status und Weiterentwicklung des IV abstimmt. Ein formales Gremium ist dafür nicht zwingend erforderlich. Der „IV-Koordinator" sollte sich mit bereits bestehenden Gremien wie z.B. dem „Architektur-Board" über gemeinsame Abhängigkeiten verständigen.

Neben obigen Rollen sind Prozesse zu definieren und in die schriftlich fixierte Ordnung zu übernehmen, wie z.B. Pflegeprozesse und Eskalationsprozesse. Damit werden Regelungen festgelegt, was zu welchem Zeitpunkt und wie gepflegt wird und wer im Informationsverbund bei konfliktären Ansichten z.B. zwischen Fachbereich und IT über Änderungen entscheidet.

Bereits zu Beginn der IV-Abbildung sind die Beauftragten bzw. die entsprechenden Funktionen im Haus zu involvieren, insb. der Informationssicherheitsbeauftragte, der Datenschutzbeauftrage, das Notfallmanagement sowie das zentrale Auslagerungsmanagement.

Mehrwert des Informationsverbunds

Der Informationsverbund hat einen Mehrwert für sich, d.h. auch ohne aufsichtsrechtliche Verpflichtung sollte jedes Institut seinen „Informationsverbund" kennen und dessen Abbildung pflegen. Nicht zuletzt trägt die genaue Kenntnis des eigenen Informationsverbunds dazu bei, auf Sicherheitszwischenfälle wie den eingangs erwähnten Cyberangriff schnell zu reagieren. Darüber hinaus geht es darum, die eigene Ist-Situation zu ordnen und transparent zu machen, um wichtige Erkenntnisse aus deren Analyse für einen wirtschaftlichen Geschäftsbetrieb zu

generieren. Nicht zuletzt soll durch einen geordneten Datenhaushalt auch die Steuerung der ORG/IT verbessert werden. So kann der Informationsverbund in folgenden, beispielhaften Situationen einen wesentlichen Mehrwert stiften:

- Der Informationsverbund schafft Transparenz über die Ist-Anwendungslandschaft als Teil der IT-Architektur und dient damit als Ausgangsbasis für die Entwicklung von IT-Architekturzielbildern.
- Der Informationsverbund fordert die Klärung von Verantwortlichkeiten für jede Anwendung und jedes Stück Infrastruktur – dies schafft Klarheit in der Zusammenarbeit zwischen Fachbereichen und IT.
- Die Abbildung des Informationsverbunds kann als Informationsbasis für die Überprüfung von IT-Strategien, und damit auch von Geschäftsstrategien, genutzt werden. Analysen des Informationsverbunds können wichtige Erkenntnisse liefern, um die Wirksamkeit von strategischen Maßnahmen und deren Ressourcen-Einsatz zu überprüfen sowie um mögliche Anpassungsbedarfe abzuleiten.

Fazit

Die Abbildung des Informationsverbunds ist aufsichtsrechtlich für Finanzdienstleister wie Banken und Versicherungen gefordert. Neben der reinen Dokumentation der relevanten IV-Elemente sind auch die Zusammenhänge zwischen den Elementen transparent zu machen. Die Aufsichtsbehörden fordern eine integrierte Sicht auf den Informationsverbund – ein Silo-Denken in einzelnen Kategorien führt i.d.R. zu Nachfragen oder ggf. zu Feststellungen.

Der Mehrwert der Abbildung des Informationsverbunds geht jedoch über das Aufsichtsrechtliche hinaus – der Nutzen besteht in der Transparenz und Strukturierung der gesamten schützenswerten Informationen und der Mittel zur Informationsverarbeitung.

Prinzipiell steht jeder einzelne Mitarbeiter im Unternehmen in der Verantwortung den Informationsverbund zu schützen. Dazu ist ein gutes Verständnis erforderlich, was der Informationsverbund überhaupt genau darstellt. Bei informationssicherheitsrelevanten Zwischenfällen oder im Notfall zahlt sich eine gute Kenntnis des Informationsverbunds aus, um schnell betroffene Teile des Informationsverbunds zu identifizieren und Gegenmaßnahmen einzuleiten. Die Vorbereitung auf und das Bestehen von Sonderprüfungen der Aufsichtsbehörden ist allenfalls als Zwischenziel zu sehen – die eigentliche Prüfung ist der reale Ernstfall selbst.

Kristian Buric ist Manager bei Eurogroup Consulting und Experte für IT-Management sowie Asset und Wealth Management. Seine Projektexpertise umfasst u.a. Fragestellungen zu Compliance, Aufbau- und Ablauforganisationen und Effizienzsteigerungen. Er ist diplomierter Ökonom sowie geprüfter Finanzanalyst (CFA, CFM) und Risikomanager (FRM).

Bisher erschienen:

#1 Dr. Marco Weiß – *Welt und Wesen des Datenmanagements*; September 2020

#2 Mario Kubik – *„DLT" – Potenzial zur Zukunftstechnologie?*; November 2020

#3 Jonathan Misler – *Verwendung von Daten und Modellen in datengetriebenen Geschäftsmodellen*; Januar 2021

#4 Johannes Bänsch – *Data Analytics und die Cloud*; März 2021

#5 Kurt Tanneberger – *Ja, wo sind sie denn? – Daten im IT-Betrieb*; Mai 2021

#6 Thomas Tiebor – *Data Governance als Fundament guten Datenmanagements;* Juli 2021

#7 Dr. Marco Weiß – *Artificial Intelligence – Nature or Nurture?*; September 2021

#8 Binjamin Sancar, Hermann Sgardelli – *Vertriebschancen in einer Bank durch Nutzung ihrer Daten und ihres Ökosystems;* November 2021

#9 Abdalla El Kadi – *Datenvisualisierung – eine Geschichte in Bildern;* Januar 2022

#10 Carsten Kuhlmann – *Kundenfokussierung: Daten und Technik*; März 2022

#11 Luca Winters – *CIEM – Cloud Infrastructure Entitlements Management*; Mai 2022

#12 Kristian Buric – *Der Informationsverbund - Daten (nur) für die Aufsicht?*; Juli 2022

#13 Stefan Bauer – *Aufbau eines SOC (Security Operations Center) als Kommandozentrale zur Cyberabwehr*; September 2022

#14 Thomas Tiebor – *Der Charme von IT-Datenarchitekturmustern;* November 2022

#15 Dr. Marco Weiß – *Citius, Altius, Fortius – Daten im Sport*; Januar 2023

#16 Simon Wilmerding – *Daten statt (nur) Bauchgefühl – Mit Datenanalysen den War for Talent gewinnen*; März 2023

#17 Kay Helbig – *ESG-Berichterstattung bei Versicherungen*; Mai 2023

#18 Dr. Marco Weiß – *Daten und Modelle in der 7. MaRisk-Novelle*; Juli 2023

#19 Fabio Giacomo Müller – *Softwareeinführungsprojekte im internationalen Kontext*; September 2023

#20 Stefan Bauer – *Digital Operational Resilience Act (DORA): Wie hoch wird die nächste Welle der Regulierung?*; November 2023

#21 Prof. Dr. Hans-Gert Penzel – *Tokenisierung von Vermögenswerten: Wie die Zukunft des Eigentums aussehen wird*; Januar 2024

Über den DataNavigator

Unterschiedliche Autoren beleuchten in der Reihe DataNavigator die vielfältigen Facetten des Datenmanagements und zeigen Ihnen interessante Aspekte auf.

Der DataNavigator wird von Eurogroup Consulting regelmäßig zweimonatlich herausgegeben und möchte Ihnen interessante Denkanstöße liefern. Wir freuen uns, Ihnen mit dem DataNavigator unsere Erfahrungen weiterzugeben und stehen Ihnen für die Diskussion gerne zur Verfügung!

Sie erreichen Autoren und Herausgeber bei Anregungen und Feedback unter der E-Mail-Adresse datanavigator@eurogroupconsulting.de.