Arbeitsrichtlinie Sicherheitsvorfall

VAV Versicherungs-Aktiengesellschaft

Klassifikation: Intern
Version 21.0

VAV VERSICHERUNGEN

Dokumenteneigenschaften

Titel	Arbeitsrichtlinie Sicherheitsvorfall
Version	21.0
Geltungsbereich	Siehe Geltungsbereich Richtlinie Informationssicherheit
Erstmalige Freigabe	18.12.2019
Verabschiedet durch	Daniel Fürdauer (Informationssicherheitsbeauftragter)
Klassifikation	Intern
Verantwortlicher Verantwortliche Abteilung	Daniel Fürdauer Datenschutz und Informationssicherheit
Fachlicher Ansprechpartner	Daniel Fürdauer (daniel.fuerdauer@vav.at)
Letztes Review	November 2021

Dokumentenhistorie

Version	Datum	Beschreibung der Änderung	Ersteller
19.0	18.12.2019	Ersterstellung in Anlehnung an die entsprechende Arbeitsrichtlinie der VHV in der Version 19.0.	Daniel Fürdauer
20.0	04.12.2020	In Anlehnung an die entsprechende Arbeitsrichtlinie der VHV in der Version 20.0: Redaktionelle Änderungen, Klarstellungen einzelner Formulierungen und Ergänzung einer Maßnahme zur Beweismittelsicherung (Kap. 2.3.1 und 2.3.2)	Daniel Fürdauer
21.0	06.12.2021	Änderungen in Anlehnung an die entsprechende Arbeitsrichtlinie der VHV in der Version 21.0: Kapitel 1.1: Aktualisierung der typischen Sicherheitsvorfälle Kapitel 1.2.1 Ergänzung, dass auch Daten-schutzvorfälle zu einem ISRT führen können Kapitel 2.1.4: Ergänzung der Verantwortung zu Information der Cyberversicherung und der Forensiker Kapitel 2.1.9: Reduzierung der Aufstellung des ISRT auf eine feste Gruppe Kapitel 2.2 Ergänzung der Information der Cyberversicherung Redaktionelle Änderungen in Folge der zuvor genannten Anpassungen	Daniel Fürdauer

Art der Freigabe – VHV Konzern

Version	Datum	Wesentliche Änderungen	Bestätigt von
19.0	18.12.2019	Nein	Matthias Vollmer (ISB)

20.0	10.12.2020	Nein	i.V. Ulrich Lintker (Leiter KDI)
21.0	03.12.2021	Nein	Ulrich Lintker (ISB; Leiter KDI)
Wesentliche Änderungen → Nein: Bestätigung durch ISB (VHV) → Ja: Bestätigung durch Vorstand VHV Holding			

Hinweis zur Schreibweise

Die verwendete männliche Sprachform dient der leichteren Lesbarkeit und meint immer alle Geschlechter (m/w/d). Die verkürzte Sprachform hat nur redaktionelle Gründe und beinhaltet keine Wertung.

INHALTSVERZEICHNIS

1. ÜBERSICHT

1.1. Einleitung

Um die Informationssicherheit im laufenden Betrieb aufrechtzuerhalten, ist es notwendig, die Behandlung von Sicherheitsvorfällen im Vorfeld zu regeln. Unter einem Informationssicherheitsvorfall (nachfolgend Sicherheitsvorfall) wird jedes unerwünschte Ereignis verstanden, welches Auswirkungen auf die Informationssicherheit und Datenschutz hat und in der Folge (hohe) Schäden nach sich ziehen kann. Die Betroffenheit von (geschäfts-)kritischen Prozessen kann erschwerend hinzukommen. Ein Sicherheitsvorfall liegt mithin auch dann vor, wenn noch kein Schaden eingetreten ist, aber eine präventive Reaktion erforderlich ist, um einen hohen Schaden abzuwenden. Dabei ist bei der Beurteilung eines möglichen Schadens wesentlich, auch die Eintrittswahrscheinlichkeit zu berücksichtigen.
Typische Sicherheitsvorfälle sind beispielsweise:

- Auftreten von Schadsoftware z. B.:
  - Kryptotrojaner (z.B. Ransomware)
  - Kryptominer
- Verteilung von Schadsoftware durch die VAV
- Überlastungsangriff auf IT-Systeme (DDos)
- kriminelle Handlungen z. B.:
  - Datendiebstahl / Datenabfluss
  - Datenmanipulation
  - SPAM-Versand durch VAV
  - „CEO-Fraud“
  - Vorsätzliche Beeinflussung von bereitgestellten IT-Dienstleistungen
  - APT / gezielte Angriffe auf IT-Systeme
  - De-Facing/Übernahme Website
  - Übernahme Twitter/Facebook/Youtube/Vimeo/google+-Account
  - Akten und sonstige Speichermedien gestohlen
  - Sabotage / Innentäter (Diskreditierung (falsche Spuren))
  - Erpressung von Personen z.B. aufgrund gestohlener Daten
  - Einbruch in Gebäude/Räumlichkeiten der VAV
- Technologien mit schweren Sicherheitslücken (z. B. Spectre/Meltdown)
- Gebrochene Kryptoverfahren
- Unautorisierte Veröffentlichung von Informationen oder Kundendaten
- Verlust zentraler Schlüssel

Sicherheitsvorfälle können ebenfalls aufgrund einer Schnittstelle zu Dienstleistern oder Vertriebspartnern entstehen, sofern diese selbst Opfer eines Sicherheitsvorfalls sind. Daher sind bei Sicherheitsvorfällen bei diesen insbesondere Auswirkungen auf die VAV durch z.B. E-Mails, Schnittstellen und Zugangsdaten zu IT-Systemen zu prüfen.

Solche Sicherheitsvorfälle können zum Beispiel ausgelöst werden durch:

- Missbrauch von Rechten
- Fehlverhalten von Benutzern, Administratoren oder externen Dienstleistern, das zu sicherheitskritischen Änderungen von Systemparametern führt und gegen interne Richtlinien oder Anweisungen verstößt
- gezielte oder ungezielte Cyber-Angriffe

- rasante Ausbreitung einer Schadsoftware
- Verletzung von Zugriffsrechten
- Ausfall der Zutrittsberechtigungssysteme,
- durchgeführte Änderungen an Software, Hardware oder Infrastruktur
- unzureichende Absicherung schutzbedürftiger Räume und Gebäude
- Hochwasser, Feuer, sonstige Umwelteinflüsse

Um Sicherheitsvorfälle auch bei Abwesenheit des bestellten Informationssicherheits- oder des bestellten Datenschutzbeauftragten schnell und korrekt bearbeiten zu können, sind bei einem Sicherheitsvorfall für diese Rollen die Vertretungsregelungen unter 2.2 zu beachten. Die bestellten Personen sind auch bei Abwesenheit über den Sicherheitsvorfall zu informieren.

1.2. Umgang mit Sicherheitsvorfällen

Sicherheitsvorfälle können in der gesamten Organisation oder auch bei Dritten, z. B. bei Dienstleistern, auftreten. Alle Arten von Sicherheitsvorfällen müssen angemessen behandelt werden. Die Behandlung von Sicherheitsvorfällen hängt zum einen von der Art des Vorfalls und zum anderen von dem zu erwartenden Schadenpotential und der Eintrittswahrscheinlichkeit ab. Ferner ist der Prozessablauf von dem Eingangskanal abhängig. Im Folgenden ist der Ablauf – unterteilt nach den jeweiligen Eingangskanälen und Arten von Vorfällen – dargestellt:

1.2.1. Meldung von Mitarbeitern

Sicherheitsvorfälle (mit und ohne IT-Bezug) sind von allen Mitarbeitern der VAV unverzüglich an die erste verfügbare Person mit dem Hinweis auf einen möglichen Sicherheitsvorfall zu melden:

1) Bestellter Informationssicherheitsbeauftragter
2) Bestellter Datenschutzbeauftragter
3) Ressortleiter IT/BO/FM
4) Gruppenleiter IT oder FM
5) Mitarbeiter IT oder FM
6) Sonstige fachlich qualifizierte Person

Sollte sich ein Incident mit einer IT-Störung als möglicher oder tatsächlich eingetretener Sicherheitsvorhall herausstellen, ist der Informationssicherheitsbeauftragte unverzüglich im Incident-Prozess einzubinden.
Eine Abgrenzung, wann ein Sicherheitsvorfall vorliegt, findet sich in der Richtlinie Informationssicherheit. Im Zweifelsfall sind Vorfälle zu melden, ob es sich um einen Sicherheitsvorfall handelt, entscheidet die erste verfügbare Person laut obiger Liste.
Der Melder ist gemäß Konzernrichtlinie Informationssicherheit dazu angehalten, die Meldung des Vorfalls über das im VAVcompass hinterlegte Meldeformular (https://compass.vav.at/dam/jcr:a6a9ac3e-b049-46bb-8c9e-ed56982b7a1b/Meldeformular_Datenschutz_und_Informationssicherheit_18.0.docx) abzugeben.
Sofern die Meldung ohne Formular eingeht, wird der Melder nachträglich um die Befüllung des Meldeformulars gebeten. Bei Sicherheitsvorfällen, die im Rahmen von Incidents erfasst und dokumentiert wurden, kann auf das Meldeformular verzichtet werden. Anhand der Informationen im Meldeformular oder Incident wird mithilfe einer einheitlichen Bewertungsmatrix eine Erstbewertung

des Vorfalls durchgeführt werden und zwar dahingehend, ob das eingetretene Ereignis ein „niedriges“, „mittleres“ oder „hohes“ Schadenpotential gemäß der Wesentlichkeitsskalen hat. Die Bewertung erfolgt durch den Informationssicherheitsbeauftragten bzw. den Datenschutzbeauftragten.
Bei einem niedrigen oder mittleren Schadenpotential und einer Betroffenheit der IT oder des FM wird der Sachverhalt in den betroffenen Fachbereichen bearbeitet.
Die ordnungsgemäße Abarbeitung und Nachverfolgung der IT-Maßnahmen erfolgt über die IT bzw. das FM. Die Stabstelle Datenschutz und Informationssicherheit wird regelmäßig über den Status der Bearbeitung durch die IT bzw. das FM informiert.
Bei der Bearbeitung von Sachverhalten mit niedrigem oder mittlerem Schadenpotenzial ist es notwendig das Notfallmanagement zu informieren, wenn einer oder mehrere der folgenden Punkte erfüllt sind:

- Anzeichen, dass mehrere Arbeitsstationen / Server mit virulentem Code befallen sind und ein eindeutiges Verhaltensmuster zeigen,
- Erkennen eines Angreifers durch das IT-Personal und / oder die Systeme,
- Vorgänge / Auffälligkeiten an Sicherheitssystemen des Konzerns im Haus bzw. an den Nahtstellen zum Internet, bei denen Angreifer gezielt Schwachstellen ausgenutzt haben und so in Besitz dieser oder dessen Rechte übernommen haben (Firewalls, File- / Emailgateways),
- Verlust oder Kompromittieren von Daten,
- Verlust von Datenträgern, mobilen Endgeräten (z.B. Diebstahl Notebook aus Dienstwagen und Erlangung von Daten durch Dritte),
- IT Sonderuntersuchungen / Aktivitäten für Fraud-Fälle.

Sofern die Erstbewertung ein „hohes Schadenpotential“ ergibt, erfolgt die Aktivierung des sog. ISRT-Prozesses (mit oder ohne IT-Bezug) durch den Informationssicherheitsbeauftragten (ISB), dessen Ablauf nachfolgend unter Kapitel 2 Sicherheitsvorfallprozess bei hohem Schadenpotenzial – Fälle des ISRT beschrieben ist.
Ergibt die Prüfung, dass das Ereignis keinerlei Sicherheitsrelevanz hat, z.B. weil es sich um eine Störung im Regelbetrieb handelt, wird der Melder entsprechend informiert und auf die Regelprozesse verwiesen.
Sofern sich aufgrund der Durchsicht der Informationen des Meldeformulars oder Incident ergibt, dass bei dem gemeldeten Sicherheitsvorfall auch eine Verletzung des Schutzes personenbezogener Daten möglich ist, erfolgt auch die Bearbeitung des Vorfalls entsprechend des Data Breach Prozesses.
Ebenfalls ist es möglich, dass bei einem Datenschutzvorfall die Vertraulichkeit der Daten erheblich beeinträchtigt wird und der Datenschutzbeauftragte zur Bewältigung der Situation den ISRT nutzt. Die Abläufe des ISRT werden hiervon nicht beeinträchtigt.
Im Falle des Verlustes von IT-Equipment erfolgt eine Meldung an den IT-Support.

1.2.2. Meldung über Sicherheitslücken von externen Stellen

In der Stabstelle Datenschutz und Informationssicherheit gehen ebenfalls Meldungen von externen Stellen ein. Diese Meldungen beinhalten Sicherheitswarnungen über bekanntgewordene Sicherheitslücken und Sicherheitsvorfälle. In der Meldung ist jeweils eine Vorbewertung, z. B. des BSI, enthalten, die die Kritikalität der Sicherheitslücke bewertet und welche Präventions-/ Abhilfemaßnahmen empfohlen werden. Die Mitarbeiter der Stabstelle Datenschutz und Informationssicherheit prüfen diese Meldungen dahingehend, ob sich die jeweils genannte

Software/Hardware in der VAV im Einsatz befindet. Sofern dies der Fall ist, wird eine Erstbewertung durchgeführt. Die weitere Bearbeitung erfolgt in der IT. Ist die Sicherheitsmeldung nicht relevant, wird die Meldung durch die Stabstelle Datenschutz und Informationssicherheit dokumentiert.

1.2.3. Erkenntnisse aus internen oder externen Audits

Aus den zum Beispiel von der Stabstelle Datenschutz und Informationssicherheit durchgeführten Audits können sich ebenfalls Erkenntnisse über Sicherheitslücken ergeben. Auch in diesem Fall erfolgt die Bewertung anhand der Risikomatrix und den zuvor dargestellten Abläufen.
Anhand der Feststellungen (hohes Schadenpotential) wird der Sicherheitsvorfallprozess mit oder ohne IT-Bezug aktiviert (siehe dazu unter Kapitel 2).
Weiterhin können auch Ergebnisse aus Penetrationstests ebenfalls auf Sicherheitslücken hinweisen. Auch hier wird anhand der Risikomatrix das Schadenspotential ermittelt und gegebenenfalls der Sicherheitsvorfall-Prozess aktiviert.

1.2.4. Meldung über den Service Desk/IT Support

Wenngleich Sicherheitsvorfälle gemäß 1.2.1 Meldung von Mitarbeitern zu melden sind, kann es vorkommen, dass ein Sicherheitsvorfall direkt an den IT Support gemeldet wird. Es erfolgt hier eine Erst-Klassifizierung, ob es sich um ein sicherheitsrelevantes Ereignis handelt und eine Einbindung der Stabstelle Datenschutz und Informationssicherheit erforderlich ist. Handelt es sich um ein sicherheitsrelevantes Ereignis, so wird der Incident der Stabstelle Datenschutz und Informationssicherheit zugeleitet. Die Stabstelle Datenschutz und Informationssicherheit bewertet danach den Vorfall und priorisiert ggf. den Incident neu. Das weitere Prozedere erfolgt entsprechend dem Vorgesagten (siehe Meldung von Mitarbeitern).

1.2.5. Meldungen über das Notfallmanagement

Im Regelfall sind die Meldeprozesse und Meldeketten so ausgelegt, dass bei Vorliegen eines Sicherheitsvorfalls gemäß der o. g. Voraussetzungen die Stabstelle Datenschutz und Informationssicherheit informiert wird. Sollte es jedoch dazu kommen, dass eine Sicherheitsvorfallmeldung fälschlicherweise beim Notfallmanagement eingeht oder sich ein Sachverhalt im Notfallmanagement zu einem Sicherheitsvorfall entwickelt, informiert das Notfallmanagement die Stabstelle Datenschutz und Informationssicherheit.

2. SICHERHEITSVORFALLPROZESS BEI HOHEM SCHADENPOTENZIAL – FÄLLE DES ISRT

Um angemessen auf Vorfälle mit hohem Schadenpotential reagieren zu können, wird ein Information Security Response Team (ISRT) benötigt, welches über die zu ergreifenden Maßnahmen entscheidet, die notwendigen Schritte veranlasst und dazu beiträgt, Schäden vom Unternehmen abzuwenden.
Die Aktivierung des ISRT durch den ISB sowie die einzelnen Aktivitäten im Rahmen dieses Prozesses sind in der nachfolgenden Prozessübersicht dargestellt – unterteilt nach IT- und Non-IT-Vorfällen.

2.1. Rollen

Im Sicherheitsvorfallprozess mit einem hohen Schadenpotential sind folgende Funktionen involviert, die die nachstehend aufgeführten Aufgaben, Befugnisse und Verantwortungen im Rahmen des hier beschriebenen Sicherheitsvorfallprozesses innehaben:

2.1.1. Informationssicherheitsbeauftragter (ISB)

Aufgaben und Verantwortung:
Die Aufgaben des ISB ergeben sich aus der Funktionsbeschreibung. Im Falle eines Sicherheitsvorfalls führt der ISB die finale Bewertung des Sicherheitsvorfalls durch und entscheidet darüber, ob der ISRT-Prozess ausgelöst wird. Er ist dafür zuständig, die Einbindung der benötigten Funktionen/Personen/Gremien/Prozesse im Sicherheitsvorfallprozess sicherzustellen. Er leitet das ISRT. Der ISB bildet die Schnittstelle zum Lagezentrum (soweit aktiv). Er stimmt mit dem Lagezentrum (soweit aktiv) und den Risikoverantwortlichen eine angemessene Strategie und Maßnahmen zur Schadenvermeidung-/minimierung bzw. beseitigung ab und leitet die dafür notwendigen Maßnahmen über die bestehenden Prozesse ein und überwacht deren Umsetzung.
Der Informationssicherheitsbeauftragte übernimmt die Kommunikation in Richtung der Geschäftsleitung, solange kein Notfall im Sinne der Definition des Notfallmanagements vorliegt. Ab Vorliegen eines Notfalls übernimmt der Leiter der Abteilung Controlling & Risikomanagement die Kommunikation mit der Geschäftsleitung. Der Informationssicherheitsbeauftragte informiert ggf. die Cyberversicherung, falls dies erforderlich ist und nicht schon durch eine andere Stelle erfolgt ist.
Befugnisse / Kompetenzen:
Der ISB entscheidet über die Einberufung des ISRT.
Sollte der Ressortleiter IT/BO/FM und dessen Vertreter in Ausnahmefällen nicht erreichbar sein, kann der ISB bei nicht aufschiebbaren Entscheidungen eine Festlegung treffen. Die Entscheidung und die ergriffenen Maßnahmen werden dem Ressortleiter IT/BO/FM und dessen Vertreter parallel per E-Mail mitgeteilt. Er ist berechtigt, Meldungen gegenüber der Cyberversicherung abzugeben und zur Beauftragung der Forensiker.

2.1.2. IT-Security Management

Aufgaben und Verantwortung:
Mitarbeiter des IT-Security-Managements können Teil des ISRT im Falle von Sicherheitsvorfällen mit IT-Bezug sein und den ISB bei der Auswahl und der Initiierung von IT-Sicherheitsmaßnahmen sowie bei der Koordination und Dokumentation beraten.

2.1.3. Datenschutzbeauftragter

Aufgaben und Verantwortung:
Der Datenschutzbeauftragte berät hinsichtlich der datenschutzrechtlichen Auswirkungen (z.B. betreffend Melde- und Benachrichtigungspflichten) sowie bei der Auswahl von Abhilfemaßnahmen unter Berücksichtigung der datenschutzrechtlichen Anforderungen. Der Datenschutzbeauftragte kann weiterer Personen zur Erfüllung seiner Aufgaben hinzuziehen.
Befugnisse /Kompetenzen:
Die Befugnisse des Datenschutzbeauftragten ergeben sich aus der Funktionsbeschreibung. Er erstellt Vorschläge für die Meldungen gegenüber der Aufsichtsbehörde bzw. Benachrichtigungsschreiben gegenüber den Betroffenen in Abstimmung mit dem zuständigen Fachbereich und der Unternehmenskommunikation. Er nimmt die Meldungen gegenüber der Aufsichtsbehörde im Namen der Geschäftsleitung vor.

2.1.4. Facility Management

Aufgaben und Verantwortung:
Das Facility Management bildet die Schnittstelle zu den externen Dienstleistern des Facility Managements. Zudem ist das Facility Management für die unmittelbare Kommunikation an das Notfallmanagement bei der Identifikation von Störungen bezüglich Gebäude/Personal verantwortlich. Die FM-Mitarbeiter, die im Rahmen des Notfallmanagements Mitglieder des Lagezentrums sind, sind ebenfalls Teil des ISRT im Falle von Sicherheitsvorfällen ohne IT-Bezug und beraten den ISB bei der Auswahl und der Initiierung von Sicherheitsmaßnahmen.
Innerhalb des ISRT übernimmt ein Mitarbeiter FM die Protokollierung aller Entscheidungen und Maßnahmen.
Befugnisse / Kompetenzen:
Der Mitarbeiter FM weist den Dienstleister zur Durchführung von Maßnahmen sowie zur Sicherstellung einer erweiterten Gebäudesicherheit/Bewachung an. Der Abteilungsleiter und die Mitarbeiter des Facility Management sind bevollmächtigt, eine kurzfristige Durchsetzung des Hausrechts, auch unter Einbezug von behördlicher Unterstützung, sicherzustellen (z.B. Erteilung eines Hausverbots).

2.1.5. Notfallmanager

Aufgaben und Verantwortung:
Das Notfallmanagement koordiniert die Tätigkeiten mit weiteren Mitgliedern des Lagezentrums bezüglich BCM, ITSCM und Facility Management.
Befugnisse / Kompetenzen:
Gemäß Konzernrichtlinie BCM ist der Notfallmanager vom Vorstand der VAV bevollmächtigt Erstmaßnahmen autark einzuleiten und besitzt das Direktionsrecht, um deren Umsetzung durchzusetzen. Er kann ad-hoc Maßnahmen treffen, um weitere Schäden von dem Unternehmen abzuwenden.

2.1.6. Lagezentrum

Aufgaben und Verantwortung:
Die Mitglieder des Lagezentrums ergeben sich aus der Geschäftsordnung des Krisenstabs.
Bei einer Störung der Infrastruktur oder der IT (INF Prio 2) kann durch das Notfallmanagement der Notfall ausgerufen und das Lagezentrum aktiviert werden. Das Lagezentrum ist ein virtuelles Team zur Bewältigung von Störungen. Wenn sowohl das Lagezentrum als auch das ISRT aktiviert wurden, kann das ISRT über das Lagezentrum auf Ressourcen zugreifen, die von diesem primär genutzt werden.
Befugnisse / Kompetenzen:
Das Lagezentrum legt die Behandlungsstrategie im Falle eines Notfalls fest.

2.1.7. Mitarbeiter IT / Manager on Duty (MoD)

Aufgaben und Verantwortung:
Der Mitarbeiter IT bildet die Schnittstelle zur IT. 2 Mitarbeiter IT sind Mitglied des ISRT bei einem IT-Sicherheitsvorfall.
Innerhalb des ISRT übernimmt ein Mitarbeiter IT die Protokollierung aller Entscheidungen und Maßnahmen.
Befugnisse/Kompetenzen:
Der Mitarbeiter IT koordiniert die Aktivitäten der IT. Er (de)eskaliert Incidents in der IT.

2.1.8. Ressortleiter IT/BO/FM

Aufgaben und Verantwortung:
Entscheidungen über einzuleitende Maßnahmen mit Auswirkungen auf den Geschäftsbetrieb auf Basis der Empfehlungen des ISRT.
Im Falle von IT-Vorfällen und Non-IT-Vorfällen im Ressort IT/BO/FM trifft der RL IT/BO/FM bzw. dessen Vertreter die notwendigen Entscheidungen. Im Falle von Non-IT-Vorfällen, die nicht in die Zuständigkeit des Ressorts IT/BO/FM fallen, entscheidet der zuständige Ressortvorstand bzw. dessen Vertreter.
Sofern der Krisenstab einberufen werden muss (in Notfällen), entscheidet dieser entsprechend der Geschäftsordnung des Krisenstabs.
Befugnisse /Kompetenzen:
Die Befugnisse und Kompetenzen entsprechen denen im Regelbetrieb.

2.1.9. Information Security Response Team (ISRT)

Die Anzahl der ISRT-Mitglieder ist bewusst klein zu halten. Die Mitglieder sollten aufgrund ihrer Aufgaben im Fall eines Sicherheitsvorfalles folgende Eigenschaften haben:

- Integrität
- Zuverlässigkeit
- Kommunikationsfähigkeit
- Teamfähigkeit
- Stresstoleranz
- Ökonomisches Denken
- Analytisches Denkvermögen
- Entscheidungsfähigkeit

Aufgaben und Verantwortung:
Das ISRT hat eine koordinierende Funktion und soll die schnelle (strategische und taktische) Entscheidungsfindung im Falle von Sicherheitsvorfällen mit hohen Schadenpotential ermöglichen. Das ISRT ist ein virtuelles Team und setzt sich bei einem IT-Sicherheitsvorfall aus folgenden Rollen zusammen:

- ISB
- DSB
- 2 Mitarbeiter IT (inkl. Protokollführung)

Bei einem Non-IT-Sicherheitsvorfall aus folgenden Rollen:

- ISB
- DSB
- 2 Mitarbeiter FM (inkl. Protokollführung)

Das Team kann bei Bedarf durch den ISB um weitere Funktionen erweitert werden, z. B. Person des IT-Security Managements, Abteilungsleitung Compliance & Recht, Ressortleiter IT/BO/FM, Gruppenleiter EK&FM, Unternehmenskommunikation (UK), Personal, Mitarbeiter der betroffenen Fachbereiche. Darüber hinaus kann der Notfallmanager als Beobachter im ISRT teilnehmen. Die Aufgaben im Team ergeben sich aus den Stellen- und Funktionsbeschreibungen der einzelnen Beteiligten sowie den hier erfolgten Konkretisierungen. Der ISB leitet das ISRT und ist die Schnittstelle zum Lagezentrum (soweit aktiv).
Befugnisse/Kompetenzen:
Das ISRT legt eine Handlungsstrategie zur Bewältigung des Sicherheitsvorfalls fest. Die Entscheidung trifft der Ressortleiter IT/BO/FM in Abstimmung mit dem ISRT. Das ISRT ist befugt Maßnahmen zur Erkennung und Analyse des Sicherheitsvorfalls anzuweisen sowie die Beauftragung von Forensikern zu veranlassen.

2.1.10. Geschäftsleitung

Aufgaben und Verantwortung:
Die Geschäftsleitung trifft Entscheidungen über einzuleitende Maßnahmen mit Auswirkungen auf den Geschäftsbetrieb auf Basis der Empfehlungen des ISRT.
Im Falle von IT-Vorfällen und Non-IT-Vorfällen im Ressort IT/BO/FM trifft der RL IT/BO/FM bzw. dessen Vertreter die notwendigen Entscheidungen. Im Falle von Non-IT-Vorfällen, die nicht in die Zuständigkeit des Ressorts IT/BO/FM fallen, entscheidet der zuständige Ressortvorstand bzw. dessen Vertreter.
Sofern der Krisenstab einberufen werden muss (in Notfällen), entscheidet dieser entsprechend der Geschäftsordnung des Krisenstabs.
Befugnisse /Kompetenzen:
Die Befugnisse und Kompetenzen entsprechen denen im Regelbetrieb.

2.2. Vertretungsregelungen

Um Sicherheitsvorfälle auch bei Abwesenheit des bestellten Informationssicherheits- oder des bestellten Datenschutzbeauftragten schnell und korrekt bearbeiten zu können, sind bei einem Sicherheitsvorfall für diese Rollen die folgenden Vertretungsregelungen zu beachten. Die bestellten Personen sind auch bei Abwesenheit über den Sicherheitsvorfall zu informieren.
Es übernimmt die jeweils höchstgereihte verfügbare Person die entsprechende Rolle.

2.2.1. Vertretungsregelung Informationssicherheitsbeauftragter

1) Bestellter Datenschutzbeauftragter
2) Ressortleiter IT/BO/FM
3) Gruppenleiter IT oder FM
4) Mitarbeiter IT oder FM
5) AL der Fachabteilung(en), in der der etwaige Sicherheitsvorfall aufgetreten ist
6) Sonstige fachlich qualifizierte Person

2.2.2. Vertretungsregelung Datenschutzbeauftragter

1) Bestellter Informationssicherheitsbeauftragter
2) AL Compliance & Recht
3) AL IT, BO, FM
4) AL oder Datenschutzexperte der Fachabteilung(en), in der der etwaige Sicherheitsvorfall aufgetreten ist
5) Sonstige fachlich qualifizierte Person (insbesondere Datenschutzexperten)

2.3. Aktivierung des ISRT

ZWISCHENABSCHNITT		
1.	**Auslöser zur Aktivierung des ISRT** Ergibt sich anhand der Risikobewertung der IT-Security bzw. des ISB oder ggf. durch die Beurteilung des DSB ein hohes Schadenpotential, aktiviert der ISB den Sicherheitsvorfall-Prozess. Der ISB informiert alle ISRT-Mitglieder (festen Mitglieder (ISB, DSB, 2 Mitarbeiter IT bzw. FM) und weitere notwendige Ressourcen) und ruft diese zusammen. Die Aktivierung erfolgt telefonisch oder im persönlichen Gespräch. Bei Nicht-Erreichen wird der Vertreter kontaktiert. Die Kontaktdaten werden an zentraler Stelle hinterlegt und regelmäßig aktualisiert. Für jeden Vorfall wird ein Arbeitsverzeichnis unter „U:\Ereignisse-Informationssicherheit\ISRT“ angelegt.	ISB
2.	**Information an den Notfallmanager** Der ISB informiert den Notfallmanager über die Aktivierung des ISRTs (primär telefonisch, alternativ per Mail) Der Notfallmanager informiert den ISB, wenn das Lagezentrum bereits aktiviert wurde oder wird.	ISB / Notfallmanagement
3.	**Information an die Cyberversicherung** Der RL IT/BO/FM oder der ISB informiert die Cyberversicherung über den vertraglich geregelten Meldeweg. Die Einordnung der Versicherung bzgl. des Eintretens eines Versicherungsfalles sowie die Aktivierung der vertraglichen Incident Response werden dem ISRT mitgeteilt.	RL IT/BO/FM / ISB
4.	**Einbinden weiterer relevanter Rollen** Das ISRT prüft, ob weitere Funktionen für die Behandlung des Sicherheitsvorfalls relevant sind und bindet diese in das ISRT mit ein. Dies können zum Beispiel folgende Rollen sein: Person des IT-Security Managements, Abteilungsleitung Compliance & Recht, Ressortleiter IT/BO/FM, Gruppenleiter EK&FM, Unternehmenskommunikation (UK), Personal, Mitarbeiter der betroffenen Fachbereiche	ISB

Tabelle 1: Aktivierung des ISRT

2.4. Behandlung des Sicherheitsvorfalls

Der weitere Prozessablauf richtet sich danach, ob es sich um einen Sicherheitsvorfall mit oder ohne IT-Bezug handelt und ob das Lagezentrum aktiv ist.

2.4.1. Sicherheitsvorfall mit IT-Bezug und Lagezentrum ist aktiv

ZWISCHENABSCHNITT		
5.	**Integration des ISRT in das Lagezentrum** Wenn das Lagezentrum vom Notfallmanagement bereits aktiviert wurde oder es im Laufe des Vorfalls aktiviert wird, wird der ISB in das Lagezentrum einbezogen. Er fungiert als Schnittstelle zwischen ISRT und Lagezentrum. Das Lagezentrum kann präventiv einberufen werden ohne dass ein Notfall vorliegt.	Notfallmanager/ISB
6.	**Bewertung der Auswirkungen und Ableiten von Optionen** Das ISRT ermittelt die Auswirkungen, die vom Sicherheitsvorfall ausgehen und leitet mögliche Optionen zur Behandlung ab. Hierzu sind ggf. weitere Detailinformationen, z.B. der IT oder dem Dienstleister einzuholen.	ISRT
	Alle Aktivitäten und Entscheidungen werden protokolliert/dokumentiert.	Mitarbeiter IT
	Der ISB informiert den Notfallmanager laufend über die ermittelten Auswirkungen sowie mögliche Handlungsoptionen. Die Meldung an das Notfallmanagement erfolgt in direkter Kommunikation per Telefon oder im persönlichen Gespräch sowie in unmittelbarer nachgelagerter schriftlicher Information.	Notfallmanager/ISB
7.	**Festlegung der Strategie** Auf Basis der zuvor getroffenen Bewertungen erfolgt die Festlegung einer Risikobehandlungsstrategie. Das Lagezentrum / ISRT und die IT bzw. der relevante IT-Dienstleister oder Fachbereiche stimmen gemeinsam die Umsetzung der einzuleitenden Maßnahmen ab.	Lagezentrum/ISB
	Die finale Entscheidung über die Umsetzung der Sofort-Maßnahme liegt beim Ressortleiter IT/BO/FM.	RL IT/BO/FM
	Mögliche Maßnahmen können sein (Beispiele):	
	• Anweisung zur Ermittlung, Sammlung, Erfassung und Aufbewahrung von Informationen, die als Beweismaterial dienen können.	ISB
	• Trennung der betroffenen IT-Systeme vom Netz	Mitarbeiter IT
	• Sicherung von relevanten Daten und Protokollen zum Sicherheitsvorfall	Mitarbeiter IT
	• Untersuchung aller betroffenen Systeme auf Veränderungen (Manipulationen) am Betriebssystem, an Applikationen, an Konfigurationen und an Benutzerdaten	Mitarbeiter IT

ZWISCHENABSCHNITT		
	• Einschalten von Forensik-Dienstleistern	ISB
	• Änderung relevanter Kennwörter und Überwachung des Netz-werkverkehrs	Mitarbeiter IT
	• Einbindung der Anwender für Funktionstests bei der Wiederherstellung	Mitarbeiter IT
	• Wiederherstellung von Datenbeständen zum festgelegten Zeitpunkt	Mitarbeiter IT
	• Kontaktaufnahme zu Dienstleistern	FB/Risikoverantwortlicher
	• Information von Strafverfolgungsbehörden und FMA und/oder Geltendmachung zivilrechtlicher Ansprüche	CR
	• Information der Datenschutzbehörde	DSB
	• Information der VAV und der Öffentlichkeit bei schwerwiegenden Sicherheitsvorfällen	UK
	• Information der Mitarbeiter	PER
8.	**Kommunikation an Geschäftsleitung** Das Notfallmanagement informiert den Leiter Controlling & Risikomanagement, dieser führt im Falle eines Notfalls die Abstimmungen mit der Geschäftsleitung durch.	Leiter Controlling & Risikomanagement
9.	**Initialisieren eines IT PRIO Prozesses** Mit der Umsetzung der festgelegten IT-Maßnahmen wird ein Mitarbeiter IT beauftragt und koordiniert im Weiteren deren Durchführung. Er hält den Umsetzungsstand nach und informiert laufend das Lagezentrum und das ISRT. Die Umsetzung von IT- Maßnahmen erfolgt in der IT. Sofern ein Change notwendig ist, wird dieser über den Changemanagement-Prozess der IT bzw. des IT-Dienstleisters durchgeführt.	Lagezentrum/ISRT/ Mitarbeiter IT
10.	**Überwachung der Maßnahmenumsetzung** Das Lagezentrum und das ISRT erhalten regelmäßig über einen Mitarbeiter IT ein aktualisiertes Lagebild. Falls die umgesetzten Maßnahmen nicht umgesetzt werden können oder nicht wirksam sind, finden erneut die vorherigen Prozessschritte statt. Hierzu stimmt sich der ISB mit dem ISRT und dem Lagezentrum ab.	Mitarbeiter IT ISB
11.	**Dokumentation der Maßnahmenumsetzung** Die Umsetzung der Maßnahmen erfolgt in der IT und wird dort protokolliert. Dies betrifft auch die ergriffenen Maßnahmen. Weiterhin werden die Entscheidungen und Maßnahmen des ISRT dokumentiert und in einem Abschlussbericht zusammengefasst.	IT ISRT

ZWISCHENABSCHNITT		
12.	**Erstellung eines Abschlussberichtes** Der gesamte Sicherheitsvorfall wird zeitnah im Rahmen eines Abschlussberichts zusammengefasst und der Geschäftsleitung und den betroffenen Parteien zur Verfügung gestellt. Entscheidungen über langfristige Maßnahmen werden dabei lediglich aufgezeigt, deren Umsetzung aber nicht abgewartet.	ISB

Tabelle 2: Sicherheitsvorfall mit IT-Bezug und Lagezentrum ist aktiv

2.4.2. Sicherheitsvorfall mit IT-Bezug und Lagezentrum ist nicht aktiv

ZWISCHENABSCHNITT		
5.	**Bewertung der Auswirkungen und Ableiten von Optionen** Das ISRT ermittelt die Auswirkungen, die vom Sicherheitsvorfall ausgehen und leitet mögliche Optionen zur Behandlung ab. Hierzu sind ggf. weitere Detailinformationen, z. B. der IT oder dem Dienstleister einzuholen.	ISRT
	Alle Aktivitäten und Entscheidungen werden protokolliert/dokumentiert.	Mitarbeiter IT
6.	**Festlegung der Strategie und der erforderlichen Maßnahmen** Auf Basis der zuvor getroffenen Bewertungen erfolgt die Festlegung einer Risikobehandlungsstrategie. Das ISRT und die IT bzw. der relevante IT-Dienstleister oder Fachbereiche stimmen gemeinsam die Umsetzung der einzuleitenden Maßnahmen ab.	ISB
	Die finale Entscheidung über die Umsetzung der Sofort-Maßnahme liegt beim Ressortleiter IT/BO/FM. Mögliche Maßnahmen können sein (Beispiele):	RL IT/BO/FM
	• Anweisung zur Ermittlung, Sammlung, Erfassung und Aufbewahrung von Informationen, die als Beweismaterial dienen können.	ISB
	• Trennung der betroffenen IT-Systeme vom Netz	Mitarbeiter IT
	• Sicherung von relevanten Daten und Protokollen zum Sicherheitsvorfall	Mitarbeiter IT
	• Untersuchung aller betroffenen Systeme auf Veränderungen (Manipulationen) am Betriebssystem, an Applikationen, an Konfigurationen und an Benutzerdaten	Mitarbeiter IT
	• Einschalten von Forensik-Dienstleistern	ISB
	• Änderung relevanter Kennwörter und Überwachung des Netzwerkverkehrs	Mitarbeiter IT
	• Einbindung der Anwender für Funktionstests bei der Wiederherstellung	Mitarbeiter IT
	• Wiederherstellung von Datenbeständen zum festgelegten Zeitpunkt	Mitarbeiter IT
	• Kontaktaufnahme zu Dienstleistern	FB/Risikoverantwortlicher
	• Information von Strafverfolgungsbehörden und FMA und/oder Geltendmachung zivilrechtlicher Ansprüche	CR
	• Information der Datenschutzbehörde	DSB
	• Information der VAV und der Öffentlichkeit bei schwerwiegenden Sicherheitsvorfällen	UK

ZWISCHENABSCHNITT		
	• Information der Mitarbeiter	PER
7.	**Kommunikation an Geschäftsleitung** Der ISB informiert die Geschäftsleitung und stimmt die Vorgehensweise mit dieser ab.	ISB
8.	**Initialisieren eines IT PRIO Prozesses** Mit der Umsetzung der festgelegten IT-Maßnahmen wird ein Mitarbeiter IT beauftragt. Dieser koordiniert im Weiteren deren Durchführung. Er hält den Umsetzungsstand nach und informiert laufend das ISRT. Die Umsetzung von IT- Maßnahmen erfolgt in der IT. Sofern ein Change notwendig ist, wird dieser über den Changemanagement-Prozess der IT bzw. des IT-Dienstleisters durchgeführt.	Mitarbeiter IT
9.	**Überwachung der Maßnahmenumsetzung** Das ISRT erhält regelmäßig über einen Mitarbeiter IT ein aktualisiertes Lagebild. Falls die umgesetzten Maßnahmen nicht umgesetzt werden können oder nicht wirksam sind, finden erneut die vorherigen Prozessschritte statt.	Mitarbeiter IT
10.	**Informieren des Notfallmanagements** Wenn die umgesetzten Maßnahmen erfolgreich waren, erfolgt eine Abschlussmeldung an das Notfallmanagement.	ISB
11.	**Dokumentation der Maßnahmenumsetzung** Die Umsetzung der Maßnahmen erfolgt in der IT und wird dort protokolliert. Dies betrifft auch die ergriffenen Maßnahmen. Weiterhin werden die Entscheidungen und Maßnahmen des ISRT dokumentiert und in einem Abschlussbericht zusammengefasst.	IT ISRT
12.	**Erstellung eines Abschlussberichtes** Der gesamte Sicherheitsvorfall wird zeitnah im Rahmen eines Abschlussberichts zusammengefasst und der Geschäftsleitung und den betroffenen Parteien zur Verfügung gestellt. Entscheidungen über langfristige Maßnahmen werden dabei lediglich aufgezeigt, deren Umsetzung aber nicht abgewartet.	ISB

Tabelle 3: Sicherheitsvorfall mit IT-Bezug und Lagezentrum ist nicht aktiv

2.4.3. Sicherheitsvorfall ohne IT-Bezug und Lagezentrum ist aktiv

ZWISCHENABSCHNITT		
5.	**Integration des ISRT in das Lagezentrum** Wenn das Lagezentrum vom Notfallmanagement bereits aktiviert wurde oder es im Laufe des Vorfalls aktiviert wird, wird der ISB in das Lagezentrum einbezogen. Er fungiert als Schnittstelle zwischen ISRT und Lagezentrum. Das Lagezentrum kann präventiv einberufen werden ohne dass ein Notfall vorliegt	Notfallmanagement/ISB
6.	**Bewertung der Auswirkungen und Ableiten von Optionen** Das ISRT ermittelt die Auswirkungen, die vom Sicherheitsvorfall ausgehen und leitet mögliche Optionen zur Behandlung ab. Hierzu sind ggf. weitere Detailinformationen, z. B. bei Dienstleistern einzuholen.	ISRT
	Alle Aktivitäten und Entscheidungen werden protokolliert/dokumentiert.	Mitarbeiter FM
	Der ISB informiert den Notfallmanager laufend über die ermittelten Auswirkungen sowie mögliche Handlungsoptionen. Die Meldung an das Notfallmanagement erfolgt in direkter Kommunikation per Telefon oder im persönlichen Gespräch sowie in unmittelbarer nachgelagerter schriftlicher Information.	Notfallmanagement/ISB
7.	**Festlegung der Strategie und der erforderlichen Maßnahmen** Auf Basis der zuvor getroffenen Bewertungen erfolgt die Festlegung einer Risikobehandlungsstrategie. Das Lagezentrum / ISRT und ggf. relevante Dienstleister oder Fachbereiche stimmen gemeinsam die Umsetzung der einzuleitenden Maßnahmen ab.	Lagezentrum/ISB
	Die finale Entscheidung über die Umsetzung der Sofort-Maßnahme im Ressort IT/BO/FM liegt beim RL IT/BO/FM, andere Entscheidungen beim zuständigen Ressortvorstand.	RL IT/BO/FM oder Ressortvorstand
	Mögliche Maßnahmen können sein (Beispiele):	
	• Kontaktaufnahme zu Dienstleistern	FM/FB/Risikoverantwortlicher
	• Information von Strafverfolgungsbehörden und FMA und/oder Geltendmachung zivilrechtlicher Ansprüche	CR
	• Information von Datenschutzbehörde	DSB
	• Information der VAV und der Öffentlichkeit bei schwerwiegenden Sicherheitsvorfällen	UK
	• Information der Mitarbeiter	PER

ZWISCHENABSCHNITT		
8.	**Kommunikation an Geschäftsleitung** Das Notfallmanagement informiert den Leiter Controlling & Risikomanagement, dieser führt im Falle eines Notfalls die Abstimmungen mit der Geschäftsleitung durch.	Leiter Controlling & Risikomanagement
9.	**Umsetzung von Maßnahmen** Der Fachbereich bzw. der Dienstleister führen die vereinbarten Maßnahmen zur Behandlung des Sicherheitsvorfalls durch.	Fachbereich/ Dienstleister
10.	**Überwachung der Maßnahmenumsetzung** Das Lagezentrum erhält regelmäßig vom Fachbereich/ Dienstleister ein aktualisiertes Lagebild. Falls die umgesetzten Maßnahmen nicht umgesetzt werden können oder nicht wirksam sind, finden erneut die vorherigen Prozessschritte statt. Hierzu stimmen sich das Lagezentrum mit dem ISB/ dem ISRT ab.	ISRT
11.	**Dokumentation der Maßnahmenumsetzung** Die Umsetzung der Maßnahmen ist zu dokumentieren. Dies betrifft auch die ergriffenen Maßnahmen. Weiterhin werden die Entscheidungen und Maßnahmen des ISRT dokumentiert und in einem Abschlussbericht zusammengefasst.	Fachbereich/Dienstleister ISRT
12.	**Erstellung eines Abschlussberichtes** Der gesamte Sicherheitsvorfall wird zeitnah im Rahmen eines Abschlussberichts zusammengefasst und der Geschäftsleitung und den betroffenen Parteien zur Verfügung gestellt. Entscheidungen über langfristige Maßnahmen werden dabei lediglich aufgezeigt, deren Umsetzung aber nicht abgewartet.	ISB

Tabelle 4: Sicherheitsvorfall ohne IT-Bezug und Lagezentrum ist aktiv

2.4.4. Sicherheitsvorfall ohne IT-Bezug und Lagezentrum ist nicht aktiv

ZWISCHENABSCHNITT		
5.	**Bewertung der Auswirkungen und Ableiten von Optionen** Das ISRT ermittelt die Auswirkungen, die vom Sicherheitsvorfall ausgehen und leitet mögliche Optionen zur Behandlung ab. Hierzu sind ggf. weitere Detailinformationen, z.B. bei Dienstleistern einzuholen.	ISRT
	Alle Aktivitäten und Entscheidungen werden protokolliert.	Mitarbeiter FM
6.	**Festlegung der Strategie** Auf Basis der zuvor getroffenen Bewertungen erfolgt die Festlegung einer Risikobehandlungsstrategie. Das ISRT und die ggf. relevanten Dienstleister oder Fachbereiche stimmen gemeinsam die Umsetzung der einzuleitenden Maßnahmen ab.	ISB
	Die finale Entscheidung über die Umsetzung der Sofort-Maßnahme im Ressort IT/BO/FM liegt beim RL IT/BO/FM, andere Entscheidungen beim zuständigen Ressortvorstand.	RL IT/BO/FM oder Ressortvorstand
	Mögliche Maßnahmen können sein (Beispiele):	
	• Kontaktaufnahme zu Dienstleistern	FM/FB/Risikoverantwortlicher
	• Information von Strafverfolgungsbehörden und FMA und/oder Geltendmachung zivilrechtlicher Ansprüche	CR
	• Information der Datenschutzbehörde	DSB
	• Information der VAV und der Öffentlichkeit bei schwerwiegenden Sicherheitsvorfällen	UK
	• Information an Mitarbeiter	PER
7.	**Kommunikation an Geschäftsleitung** Der ISB informiert die Geschäftsleitung und stimmt die Vorgehensweise mit dieser ab.	ISB
8.	**Umsetzung von Maßnahmen** Mit der Umsetzung der festgelegten Maßnahmen wird der Fachbereich/Dienstleister beauftragt und koordiniert im Weiteren deren Durchführung. Er hält den Umsetzungsstand nach und informiert laufend das ISRT.	Fachbereich/ Dienstleister
9.	**Überwachung der Maßnahmenumsetzung** Das ISRT erhält regelmäßig über den Fachbereich/Dienstleister ein aktualisiertes Lagebild. Falls die umgesetzten Maßnahmen nicht umgesetzt werden können oder nicht wirksam sind, finden erneut die vorherigen Prozessschritte statt.	ISRT

ZWISCHENABSCHNITT		
10.	**Informieren des Notfallmanagements** Wenn die umgesetzten Maßnahmen erfolgreich waren, erfolgt eine Abschlussmeldung an das Notfallmanagement.	ISB
11.	**Dokumentation der Maßnahmenumsetzung** Die Umsetzung der Maßnahmen ist zu dokumentieren. Dies betrifft auch die ergriffenen Maßnahmen. Weiterhin werden die Entscheidungen und Maßnahmen des ISRT dokumentiert und in einem Abschlussbericht zusammengefasst.	Fachbereich/ Dienstleister ISRT
12.	**Erstellung eines Abschlussberichtes** Der gesamte Sicherheitsvorfall wird zeitnah im Rahmen eines Abschlussberichts zusammengefasst und der Geschäftsleitung und den betroffenen Parteien zur Verfügung gestellt. Entscheidungen über langfristige Maßnahmen werden dabei lediglich aufgezeigt, deren Umsetzung aber nicht abgewartet.	ISB

Tabelle 5: Sicherheitsvorfall ohne IT-Bezug und Lagezentrum ist nicht aktiv

2.5. Abschluss des Sicherheitsvorfallprozesses

ZWISCHENABSCHNITT		
13.	**Koordinieren und Durchführen einer Lessons Learned Abstimmung** Zum Abschluss des Prozesses wird vom ISRT eine Lessons Learned Abstimmung zur Nachbereitung des Sicherheitsvorfalls mit allen Beteiligten koordiniert um folgende Themen zu prüfen und Verbesserungspotentiale zu erkennen: • Optimierung der Reaktionszeiten • Einhaltung der Meldewege prüfen und bei Bedarf schulen • Einhaltung des ISRT-Prozess • Verbesserungen am ISRT-Prozess, z. B. die Bewertung von Risiken, Mitglieder im ISRT, Abläufe des ISRT • Verbesserung der Schnittstellenaufgaben zu anderen Prozessen • Etablierung von präventiven Maßnahmen gegen ähnliche Sicherheitsvorfälle • Bei Angriffen: Analyse der Tätermotivation um Bedrohungen und Gefährdungen besser einzuschätzen • Bei menschlichen Fehlhandlungen: Berücksichtigung bei der Sensibilisierung und Schulung Über die Lessons Learned wird durch den ISB ein Protokoll erstellt und der gesamte Sicherheitsvorfall im Jahres- und Quartalsbericht erwähnt.	ISB

Tabelle 6: Abschluss des Sicherheitsvorfallprozesses