Parasol Island

Business Continuity Management Richtlinie

Dateiname:	02_04_PSL_ISMS_Business_Continuity_Management_v00.10_jH
Dokumentenebene:	02_Richtlinie
Erstellt von:	Philip Hansen
Version:	00.10
Status:	Freigegeben
Letzte Aktualisierung am/von:	08.11.2017 | Justus Heinser
Exportiert am:	08.11.2017
Prüfungsintervall:	Jährlich
Letzte Prüfung:	08.11.2017
Sicherheitsklassifizierung:	Intern
VDA ISA Referenz:	17.1

Version	Datum	Autor	Änderung
00.01	30.08.2017	Philip Hansen	Erstellung
00.02	14.09.2017	Justus Heinser	Ergänzung
00.10	08.11.2017	Justus Heinser	Finalisierung

Parasol Island

Inhaltsverzeichnis

Parasol Island

1. Ziel der BCM Richtlinie

Die BCM Richtlinie soll Informationen zum Umgang mit Notfällen aufzeigen, um eine möglichst reibungslose Weiterführung oder Wiederaufnahme des Geschäftsbetriebes zu gewährleisten.
Um größere Schäden zu begrenzen bzw. diesen vorzusorgen, ist eine zügige und effiziente Behandlung von Sicherheitsvorfällen, die zum Ausfall von IT-Systemen führen, notwendig.
Ein Notfallvorsorgekonzept hat zum Ziel, die Geschäftstätigkeit während eines Ausfalls eines IT-Systems oder einer IT-Anwendung aufrechtzuerhalten und sicherzustellen (Business Continuity) sowie die Betriebsfähigkeit innerhalb einer tolerierbaren Zeitspanne wiederherzustellen (Business Recovery).

Dabei sind nicht nur die technischen Maßnahmen zum Wiederanlauf zu beachten. Besonders wichtig ist die Planung im Vorfeld, um Notfälle zu verhindern oder zumindest die Auswirkungen begrenzen zu können. Zur Vorbereitung gehören die Dokumentation von Verfahren und Maßnahmen sowie organisatorische Regelungen. Im Notfall muss es z. B. Verantwortliche mit klaren Kompetenzen geben. Zu einer guten Vorbereitung gehören ebenso Notfallschulungen und -übungen sowie eine stetige Pflege und Aktualisierung des Notfallvorsorgekonzeptes.

Ein Notfallvorsorgekonzept beschreibt, welche Maßnahmen zur Vorbereitung auf Notfälle unternommen werden und was im Notfall zu tun ist.

2. Definition Notfall

Der Ausfall eines IT-Systems in Folge eines Sicherheitsvorfalls kann einen großen Schaden nach sich ziehen. So kann der Ausfall eines zentralen IT-Systems zu einem Ausfall des gesamten IT-Betriebs führen. Auch der Ausfall von Komponenten der technischen Infrastruktur, beispielsweise Klimaanlage oder Stromversorgung, kann zu Störungen des IT-Betriebs führen.

Technisches Versagen muss nicht zwingend die Ursache für den Ausfall von IT-Systemen sein. Ausfälle werden oft durch menschliches Fehlverhalten (z. B. fahrlässige Zerstörung von Gerät oder Daten) oder vorsätzliche Handlungen (z. B. Diebstahl, Sabotage, Viren-Angriff) verursacht. Auch durch höhere Gewalt (wie Feuer, Blitzschlag oder Hochwasser) können hohe Schäden eintreten.

3. Verantwortlich

Ein "Notfall" sollte formal durch einen Notfall-Verantwortlichen ausgerufen werden, da schnelle Entscheidungen unabhängig von Hierarchieebenen getroffen und Mitarbeiter vielleicht außerhalb der normalen Arbeitszeit verständigt werden müssen. Auch könnten Maßnahmen, die vom normalen Arbeitsablauf abweichen und Sonderberechtigungen erfordern, notwendig werden. In Notfällen

müssen unter Umständen Beschränkungen und Sicherheitsvorkehrungen außer Kraft gesetzt werden, um ein Problem schneller lösen zu können.

In den Notfallplänen muss daher festgelegt werden, welche Aufgaben einzelne Personen im Notfall übernehmen und welche Rechte sie haben. Die beteiligten Personen und Organisationseinheiten sind dann im Notfall befugt, die ihnen übertragenen Aufgaben eigenverantwortlich durchzuführen.

4. Verhalten in Notfällen

Folgende Verhaltensregeln gelten allgemein für alle Mitarbeiter:

- Alle Mitarbeiter haben im Vorfeld die Erstellung des Notfallfallvorsorgekonzepts (z. B. Erstellung der Dokumentationen) nach Kräften zu unterstützen. Nur durch eine gute Vorbereitung ist es möglich, im Notfall Ruhe zu bewahren und nicht durch unüberlegte Handlungen den Schaden zu vergrößern.
- Unregelmäßigkeiten, die auf einen Sicherheitsvorfall hindeuten, sind gemäß den Alarmierungsplänen unverzüglich zu melden.
- Die Handlungsanweisungen für ausgewählte Schadensereignisse sind einzuhalten.
- Es sind die Anweisungen des Notfall-Verantwortlichen und etwaige spezielle Verhaltensregeln zu beachten.
- Alle Begleitumstände sind ungeschönt, offen und transparent zu erläutern, um damit Schäden zu mindern, schnell Lösungen zu finden und Erkenntnisse zur Verbesserung des IT-Sicherheitskonzepts zu gewinnen.
- Informationen über den Notfall dürfen nicht an unautorisierte externe Dritte weitergegeben werden.
- Nach einem Notfall ist der sichere Normalzustand wiederherzustellen und an der Aufarbeitung des Notfalls mitzuarbeiten.
- Das Notfallvorsorgekonzept ist stets aktuell zu halten und zu verbessern.

5. Sofortmaßnahmen

Derjenige, der einen Sicherheitsvorfall bemerkt, leitet umgehend erste Maßnahmen ein (z. B.: Alarmierung, Rechner ausschalten, Fenster schließen, ...).
Welche Verhaltensregeln bei Vorfällen gelten, muss in den Handlungsanweisungen für ausgewählte Schadensereignisse beschrieben werden.

6. Alarmierung

Die verantwortlichen Stellen, die aktiv handeln müssen, sind zu alarmieren (z. B. Feuerwehr, Administrator, Informationssicherheitsbeauftragter). Sie übernehmen dann in der Regel die weitere Untersuchung und Bewertung des Vorfalls und leiten Maßnahmen ein.

Im Vorfeld sind Alarmierungspläne zu erstellen, die die Meldewege für ausgewählte Schadensereignisse beschreiben.

Als Anhang müssen Adress- und Telefonlisten geführt werden. Relevante Telefonnummern externer Dienstleister und Behörden dürfen nicht vergessen werden, z. B.:

- Feuerwehr
- Polizei
- Notarzt
- Wasser- und Stromversorger
- Ausweichrechenzentrum
- Telekommunikationsanbieter
- IT-Techniker
- Softwarehersteller

Damit allen Mitarbeitern die Ansprechpartner bekannt sind, werden diese Listen an alle in Schriftform verteilt sowie im Intranet bereitgestellt.

7. Untersuchung und Bewertung des Vorfalls

Um einen Sicherheitsvorfall untersuchen und bewerten zu können, sind in der Regel folgende Informationen notwendig:

- betroffene IT-Komponenten (IT-Systeme und IT-Anwendungen)
- betroffene Geschäftsprozesse
- Ansprechpartner (Technik und Fachabteilung)
- Verfügbarkeitsanforderungen der IT-Komponenten
- Schutzbedarf der IT-Komponenten und der damit verarbeiteten Informationen
- möglicher Schaden: Schadensart, Schadenshöhe, Geschädigte (z. B. Kunden oder Geschäftspartner)
- mögliche Folgeschäden
- Ursache des Vorfalls (technisches Versagen, Unachtsamkeit, gezielter Angriff)
- Maßnahmen zur Behebung des Vorfalls

Um alle Informationen schnell zur Hand zu haben sind mindestens folgende Vorarbeiten nötig:

- Beschreibung und Bestand der Hard- und Software

- Schutzbedarfsfeststellung
- Zusammenstellung der Verfügbarkeitsanforderungen
- Beschreibung der Infrastruktureinrichtungen

8. Maßnahme zur Problemlösung

1. Reihenfolge der Fehlerbehebung

Bei der Behebung von Schäden sind verschiedene Aspekte zu berücksichtigen, wenn unterschiedliche Vorfälle, mehrere IT-Komponenten oder verschiedene Geschäftsprozesse betroffen sind und eine Wiederanlaufreihenfolge festgelegt werden muss.

- Bedeutung einer ausgefallenen IT-Komponente oder des betroffenen Geschäftsprozesses (Schutzbedarfsfeststellung, insbesondere Verfügbarkeitsanforderungen).
- Bewertung unterschiedlicher Schadensarten durch die Unternehmens- oder Behördenleitung
- Entsprechende Vorgaben sollten nach Möglichkeit vorab dokumentiert werden.
- Technische oder ablaufbedingte Abhängigkeiten der IT-Systeme und IT-Anwendungen voneinander.
- Es besteht die Möglichkeit, dass bestimmte Prozesse erst dann wiederhergestellt werden können, wenn andere, die als Grundlage zu sehen sind, bereits wieder funktionsfähig sind.
- Entsprechende Dokumentationen sind im Vorfeld anzufertigen.

2. Voraussetzungen für kurze Wiederanlaufzeiten

Um im Schadensfall Probleme möglichst schnell lösen zu können, müssen rechtzeitig Vorbereitungen getroffen werden:

- Erstellung von eigenen Dokumentationen und sorgfältige Archivierung von externen Dokumenten.
- Datensicherung
- Verträge mit externen Dienstleistern, Herstellern und Lieferanten
- Ersatzbeschaffungsplan für Hardware

3. Notbetrieb

Nicht immer kann jedes Problem in einer tolerierbaren Zeitspanne behoben werden (Beispiel: Reparatur eines IT-Systems dauert zu lange). In diesen Fällen ist es erforderlich, die wichtigsten Geschäftsprozesse provisorisch aufrecht zu erhalten. Verschiedene Möglichkeiten bieten sich je nach Vorfall an:

- Einschränkung des IT-Betriebs
- Um bei einem eingeschränkten IT-Betrieb die geschäftskritischen Prozesse betreiben zu können, ist für IT-Anwendungen die zur Verfügung gestellte Kapazität auf das notwendige Maß zu reduzieren.
- manuelle Ersatzverfahren:

- interne oder externe Ausweichmöglichkeiten
- Die notwendigen Dokumentationen sowie Kontaktadressen von Dienstleistern, Herstellern und Lieferanten sind im Vorfeld zusammenzustellen.

4. Informationspolitik

Unter Umständen müssen betroffene interne und externe Stellen über den Vorfall informiert werden. Dies sind insbesondere diejenigen Stellen, die direkt durch den Sicherheitsvorfall Schäden erleiden könnten, Gegenmaßnahmen ergreifen müssen oder solche, die Informationen über Sicherheitsvorfälle aufbereiten und bei der Vorbeugung oder Behebung helfen können. In Einzelfällen kann es auch notwendig sein, die Medien zu informieren.
Anweisungen für bestimmte Schadensszenarien mit den nötigen Kontaktdaten sind vorab zusammenzustellen.

5. Dokumentation

Eine Dokumentation des Notfalls ist notwendig, um für zukünftige Vorfälle zu lernen und Veränderungen an IT-Systemen und IT-Anwendungen nachvollziehen zu können. Dies ist besonders wichtig, wenn unter Zeitdruck oder mit Sonderrechten gearbeitet wurde.
Protokoll- und Log-Dateien können im Nachhinein eine wertvolle Hilfe sein und sollten daher gesichert werden.
Bei der Dokumentation sollte auch an eine mögliche Strafverfolgung gedacht werden.

6. Nachbereitung von Notfällen

Eine Nachbereitung von Notfällen hat aus zwei Gründen zu erfolgen:

Verbesserungspotentiale erkennen

Dazu sind z. B. folgende Fragen zu klären:

- Waren die Reaktionszeiten ausreichend?
- Hat die Alarmierung funktioniert oder gab es Probleme bei der Eskalation des Vorfalls?
- Wurde die Ursache des Vorfalls schnell gefunden und wurden die Auswirkungen richtig eingeschätzt?
- Waren alle Dokumentationen brauchbar und aktuell?
- Wenn es einen Täter gab: Was hat ihn motiviert?
- Was muss in Zukunft verbessert werden?

Wiederherstellung eines stabilen Normalzustandes

Nach einem Notfall ist dafür zu sorgen, dass möglichst schnell der sichere Normalzustand wieder erreicht wird. Zur Behebung des Notfalls sind unter Umständen Anwendungen, IT-Systeme oder Konfigurationen verändert oder elektronische Abläufe durch manuelle ersetzt worden.
Es kann z. B. auch erforderlich sein, Passwörter neu zu vergeben und zu verändern.

7. Revision des Notfallvorsorgekonzeptes

Das Managementsystem zur Behandlung von Sicherheitsvorfällen, und damit auch das Notfallvorsorgekonzept, muss regelmäßig auf seine Aktualität und Wirksamkeit geprüft werden. Die Notfallübungen können dabei wertvolle Erkenntnisse liefern.

Alle Maßnahmen müssen regelmäßig daraufhin überprüft werden, ob sie

- wirksam und effektiv sind,
- den betroffenen Mitarbeitern bekannt sind,
- unter Stress umsetzbar sind und
- in den Betriebsablauf integrierbar sind.

8. Datensicherungsplan

Datensicherungen sind zu erstellen, um Datenverlust vorzubeugen und Ersatz-Systeme schnell in Betrieb nehmen zu können.
Mit Hilfe eines Datensicherungsplans muss ein sachverständiger Dritter in der Lage sein, sämtliche für den Wiederanlauf einer IT-Anwendung erforderliche Software (Betriebssystemsoftware, Anwendungssoftware) und deren Daten in angemessener Zeit beschaffen und installieren zu können.
Ein Datensicherungsplan muss Auskunft geben können über:

- Datum der Datensicherung
- Datensicherungsumfang (welche Dateien/Verzeichnisse wurden gesichert)
- Datenträger, auf dem die Daten im operativen Betrieb gespeichert sind
- Datenträger, auf dem die Daten gesichert wurden
- für die Datensicherung eingesetzte Hard- und Software (mit Versionsnummer)
- bei der Datensicherung gewählten Parameter (Art der Datensicherung usw.)
- Ort der Aufbewahrung

Es ist ein Datensicherungskonzept zu erstellen und zu beachten, in dem die Datensicherung explizit geregelt wird.

9. Versicherungsschutz

Verbleibende Restrisiken sollten möglichst unter Beachtung von Kosten-Nutzen-Aspekten durch Versicherungen abgedeckt werden. Beispiele sind:

- Sachversicherungen
- Feuerversicherung
- Einbruchdiebstahlversicherung
- Transportversicherung
- Datenträgerversicherung
- Elektronik-Versicherung

Die Fachverantwortlichen sind dafür verantwortlich, dass für ihre Prozesse der Abschluss von Versicherungen untersucht wird.

10. Technische Maßnahmen

Um zu vermeiden, dass ein Sicherheitsvorfall zum Notfall wird, müssen Sicherheitsvorfälle durch technische Maßnahmen verhindert oder möglichst frühzeitig entdeckt werden.

Es gibt eine Reihe von Sicherheitsvorfällen, die mit entsprechender technischer Unterstützung automatisiert und daher frühzeitig erkannt werden können. Zu diesem Zweck sollen Detektionsmaßnahmen installiert werden.

Beispiele für solche technischen Detektionsmaßnahmen sind:

- Gefahrenmeldeanlage
- Rauchmelder
- Fernanzeige von Störungen
- Computer-Viren-Schutzprogramme
- Intrusion Detection und Intrusion Response Systeme
- Kryptographische Checksummen und digitale Signaturen

Die technischen Detektionsmaßnahmen müssen durch zusätzliche organisatorische Maßnahmen ergänzt werden (z. B. Meldewege, regelmäßige Aktualisierung und Überprüfung).

Bei der Auswahl von Detektionsmaßnahmen ist immer eine Kosten-Nutzen-Berechnung vorzulegen und die Wirksamkeit kritisch zu hinterfragen.

Die Infrastruktur (Gebäude und Räume) ist durch geeignete Maßnahmen zu sichern. Dazu gehören beispielsweise die Bereiche Zugangsschutz, Diebstahlschutz, Schutz vor Naturereignissen, Stromversorgung, Klimatisierung.

Durch eine unterbrechungsfreie Stromversorgung ist sicherzustellen, dass für hochverfügbare IT-Systeme ein kurzzeitiger Stromausfall keinen Schaden verursacht.

11. Ausbildung und Training der Mitarbeiter

Ein qualitativ hochwertiges Notfall- und Kontinuitätsmanagement greift nur dann optimal, wenn die Mitarbeiter zum einen für sicherheitsrelevante Vorfälle sensibilisiert sind und zum anderen bestmöglich für sicherheitsrelevante Vorfälle geschult werden.

Sämtliche Mitarbeiter werden in der Anwendung des Notfallvorsorgekonzeptes geschult.

12. Schutzbedarf und Verfügbarkeitsanforderungen

Es ist festzulegen, welche Geschäftsprozesse von hoher Relevanz für die Geschäftstätigkeit sind und daher ein Verlust oder die Nicht-Verfügbarkeit einen hoher Schaden bedeutet.
Der Schutzbedarf der wichtigsten IT-Anwendungen (einschließlich der verarbeiteten Informationen) und IT-Systeme ist zu bestimmen. Dabei sind insbesondere die Verfügbarkeitsanforderung festzulegen.

13. Ersatzbeschaffungsplan

Ein allgemein gültiger Ersatzbeschaffungsplan ist aufgrund der stark variierenden Projektanforderungen, Deadlines und Hard- wie auch Softwareausstattung nicht möglich. Im Notfall wird eine Gruppe aus IT-Fachkräften und Projektleitern bestimmen, welche Maßnahmen zu ergreifen sind, um eine möglichst reibungslose Fortführung oder Wiederaufnahme der aktuell laufenden Projekte zu erreichen.

14. Wiederanlaufreihenfolge

Technische oder ablaufbedingte Abhängigkeiten der IT-Systeme und IT-Anwendungen sowie deren Wichtigkeit beeinflussen die Wiederanlaufreihenfolge nach einem Ausfall eines IT-Systems oder dem Abbruch einer Anwendung. Entsprechende Zusammenhänge sind zu dokumentieren.

15. Ausweichmöglichkeiten

Angaben zu Ausweichmöglichkeiten sollten der Dokumentation der IT-Systeme beigefügt werden. Das Ausweichen auf alternative Rechenzentren, IT-Systeme, Arbeitsplätze etc. sollte in Notfallübungen ausreichend geprobt werden.

16. Interne Ausweichmöglichkeiten

Alle Fachverantwortlichen sollten prüfen, ob bei Problemen mit den standardmäßig genutzten IT-Systemen ein Ausweichen auf andere IT-Systeme möglich ist. Bei der Untersuchung von Ausweichmöglichkeiten ist insbesondere auf die technischen Anforderungen an das Ausweich-IT-System zu achten. Kompatibilität und ausreichende Kapazitätsreserven des Ausweich-IT-Systems sind Grundvoraussetzung für dessen Benutzung.

17. Externe Ausweichmöglichkeiten

Externe Ausweichmöglichkeiten sind dann heranzuziehen, wenn mit internen Ausweichmöglichkeiten die Verfügbarkeitsanforderungen nicht mehr oder nicht wirtschaftlich erfüllt werden können. Ausweichmöglichkeiten für nicht IT-spezifische Komponenten sind auch zu berücksichtigen. Beispielsweise im Bereich der Infrastruktur sind Ausweichmöglichkeiten für Serverräume in Betracht zu ziehen.

Ausweicharbeitsplätze, -Räume, -Rechenzentren etc. sind so vorzubereiten, dass im Notfall die Wechselzeit tolerierbar ist.
Größere Mengen an IT-Equipment kann über Miet- und Leasingpartner geordert werden. Diese werden über die allgemeinen Wege im Produktionsbüro organisiert, wie sie auch für normale Veranstaltungsprojekte für Kunden der Parasol Island GmbH zum Teil im Einsatz sind.
Für zusätzliche Rechenleistung sind mehrere Renderfarmen bekannt, die in der Vergangenheit bereits eingesetzt wurden.
Für die externen Ausweichmöglichkeiten ist immer auch eine Risikoeinschätzung erforderlich, um sicherzustellen, dass Informationen gemäß ihrer Sicherheitsklassifizierung behandelt werden.