

Sicherheitsvorfallkonzept

1 Definition Sicherheitsvorfall

- (1) Zwischen dem Dienstleister und der IBB werden folgende einheitliche Definitionen zur Abgrenzung von potentiellen und tatsächlichen Sicherheitsvorfällen mitsamt den notwendigen Maßnahmen definiert:

Ein Sicherheitsvorfall ist ein unerwünschtes Ereignis, das negative Auswirkungen auf Betroffene hat oder potentiell haben kann. Jedem Sicherheitsvorfall geht ein sicherheitsrelevantes Ereignis voraus. In Verbindung mit einem Sicherheitsvorfall steht die Beeinträchtigung der Schutzziele Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen, Geschäftsprozessen, IT-Diensten, IT-Systemen oder IT-Anwendungen. Falls nur das Schutzziel der Verfügbarkeit betroffen ist, geht daraus nur ein Sicherheitsvorfall hervor, wenn das Ereignis durch einen bewusst handelnden Angreifer oder grob fahrlässiges Verhalten ausgelöst wurde.

Kategorie	Schaden	Ursache	Behebung
Kategorie 3 - „geringfügige Sicherheitsvorfälle“	Kein bis sehr geringer Schaden ist zu erwarten, Keine vorsätzlichen Handlungen zu erwarten	Ursachen sind bekannt oder schnell zu erkennen	Der Vorfall kann sofort behoben werden
Kategorie 2 - „mittlere Sicherheitsvorfälle“	Ein mittlerer Schaden kann nicht ausgeschlossen werden	Die Ursachen sind nicht bekannt und es können weitere Auswirkungen nicht ausgeschlossen werden	Kann durch den Dienstleister im Regelbetrieb behoben werden
Kategorie 1 - „erhebliche Sicherheitsvorfälle“	Ein erheblicher Schaden kann nicht ausgeschlossen werden, Die Einbindung von Ermittlungsbehörden kann notwendig werden	Externe oder interne Angreifer können nicht ausgeschlossen werden	Für die Behebung der Sicherheitsvorfälle ist eine signifikante zwischen dem Dienstleister, der IBB und ggf. externe Unterstützung notwendig

Kategorie	Maßnahmen des Dienstleisters
Kategorie 3 - „geringfügige Sicherheitsvorfälle“	Behandlung nach eigenen Vorgaben des Dienstleisters.
Kategorie 2 - „mittlere Sicherheitsvorfälle“	Eindämmung der potentiellen Auswirkungen, Information der IBB gleich nach Bekanntwerden des sicherheitsrelevanten Ereignisses, Behandlung und Ursachenanalyse des Ereignisses, Fortlaufende Information der IBB über relevante Änderungen, Abschlussbericht mit Ursachenanalyse und Lösung zur zukünftigen Vermeidung
Kategorie 1 - „erhebliche Sicherheitsvorfälle“	Eindämmung der potentiellen Auswirkungen, Information der IBB gleich nach Bekanntwerden des sicherheitsrelevanten Ereignisses, Abstimmung der notwendigen Maßnahmen von der IBB, Abstimmung über die potentielle Einbindung von Ermittlungsbehörden und weiteren Experten, Behandlung und Ursachenanalyse des Ereignisses, Fortlaufende Information der IBB über relevante Änderungen, Abschlussbericht mit Ursachenanalyse und Lösung zur zukünftigen Vermeidung.

2 Vorgehen Sicherheitsvorfallbehandlung

- (1) Der Dienstleister hat folgenden internen Prozess zur Identifizierung, Eindämmung, Beseitigung und Bewertung von Sicherheitsvorfällen etabliert:

Bitte befüllen:

Beschreibung des Prozesses zur Sicherheitsvorfallbehandlung beim Dienstleister.

- (2) Der Dienstleister stellt sicher, dass bei einem Verdacht von vorsätzlichen Handlungen oder wenn schwerwiegende Auswirkungen zu erwarten sind, forensische Untersuchungen durch qualifizierte Personen zeitnah durchgeführt werden.

- (3) Über die folgende Meldekette wird sichergestellt, dass alle erforderlichen Stellen schnellstmöglich in die Behandlung der Sicherheitsvorfälle geeignet eingebunden werden:

Bitte befüllen:

Beschreibung der Meldekette beim Dienstleister und in der IBB

Hinweis: Bitte das Vorgehen bei Bekanntwerden eines Sicherheitsvorfalls beim Dienstleister beschreiben. Hierzu zählen die Schritte die bei Bekanntwerden des Sicherheitsvorfalls eingeleitet werden, bis zur Meldung des Sicherheitsvorfalls an die IBB

- (4) Der Dienstleister stellt sicher, dass etwaige Sicherheitsvorfälle zu folgenden Zeiten identifiziert werden können:

Bitte befüllen:

Zeiten zur Identifikation von Sicherheitsvorfällen durch den Dienstleister gemäß den Anforderung der IBB: Schutzbedarfsklasse „3 - hoch“ und „4 - sehr hoch“: 24/7

- (5) Der Dienstleister stellt sicher, dass zu folgenden Zeiten mit der Eindämmung und Beseitigung von Sicherheitsvorfällen begonnen wird:

Bitte befüllen:

Zeiten zur Eindämmung und Beseitigung von Sicherheitsvorfällen durch den Dienstleister gemäß den Anforderung der IBB: Schutzbedarfsklasse „3 - hoch“ und „4 - sehr hoch“: 24/7

- (6) Der Dienstleister stellt durch folgende Aktivitäten sicher, dass die etablierten Maßnahmen zur Sicherheitsvorfallbehandlung den Erwartungen entsprechend funktionieren:

Bitte befüllen:

Beschreibung der Aktivitäten durch den Dienstleister

3 Dokumentation Sicherheitsvorfälle

- (1) Folgende Inhalte werden bei sicherheitsrelevanten Ereignissen und Sicherheitsvorfällen durch den Dienstleister dokumentiert:
- Beschreibung der sicherheitsrelevanten Ereignisse und Sicherheitsvorfälle
 - Entscheidungen und Handlungen im Rahmen der Bewältigung von Sicherheitsvorfällen
 - Ursache der Sicherheitsvorfälle
 - Maßnahmen zur Vermeidung zukünftiger Sicherheitsvorfälle oder Verbesserung der Sicherheitsvorfallbehandlung
- (2) Der Dienstleister informiert die IBB umgehend, sobald potentielle Sicherheitsvorfälle gemeldet werden, die die Informationssicherheit der IBB beeinträchtigen könnten und stellt der IBB alle relevanten Unterlagen zur Verfügung. Hierunter sind mindestens die folgenden Unterlagen zu verstehen:
- Beschreibung des potentiellen Vorfalls,*
 - Protokoll der Meldungen und durchgeführten Maßnahmen,*
 - Bewertung der Auswirkungen auf die IBB,*
 - Ursachenanalyse*