|  |  |
| --- | --- |
| Version: | 1.0 |
| Status: | Freigegeben |
| Dokumentenklassifizierung: | intern |

Template "Beurteilung des Impacts von Sicherheitsmeldungen"

1. Januar 2020

Allgemeine Informationen zum vorliegenden Dokument

|  |  |  |
| --- | --- | --- |
| Bezeichnung | Inhalt | Bearbeitungshinweis |
| Eigentümer |  | [verantwortlich für die Erstellung und Pflege des Dokuments = Abteilungsleitung] |
| Autor |  | [operative Verantwortung für das Dokument] |
| Status | Freigegeben | [Einstufung des aktuellen Dokumentenstatus <Entwurf, Finaler Entwurf, Final/Freigegeben>] |
| Klassifizierung | intern | [Einstufung der Dokumentenvertraulichkeit  offen, intern, vertraulich, streng vertraulich] |
| Dokumen­tenkennung | TMP400007 | [Die Dokumenten-Kennung wird von der Dokumentenlenkung (vergeben] |
| Name des Dokuments | Template "Beurteilung des Impacts von Sicherheitsmeldungen" | [Bezeichnung des Dokuments wie auf dem Titelblatt beschrieben.] |
| Version | 1.0 | [zweistellige Versionsnummer] |
| Veröffentlichungsform | digital | [Veröffentlichungsform Papier, digital] |
| Speicherort |  | [Ablageort des Dokumentes] |
| Freigabe am | <TT.MM.YYYY> | [Datum der Freigabe durch den Eigentümer] |
| Freigabe bis | <TT.MM.YYYY> | [Datum der Freigabe bis durch den Eigentümer] |
| Revisionszyklus | Alle 1 Jahre | [Revisionszyklus alle 1, 2 Jahre] |
| Archivierungszeitraum | 5 Jahre | [Archivierungszeitraum nach Ablauf 5, 10 Jahre] |

Dokumentenhistorie

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Beschreibung | Autor | Datum |
| 0.1 | initiale Erstellung |  |  |
| 0.2 – 0.8 | draft |  |  |
| 0.9 | final draft |  |  |
| 1.0 | final/freigegeben |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Inhaltsverzeichnis

[Allgemeine Informationen zum vorliegenden Dokument 2](#_Toc87801321)

[Dokumentenhistorie 3](#_Toc87801322)

[Inhaltsverzeichnis 4](#_Toc87801323)

[Arbeitsblatt Beurteilung von Sicherheitsmeldungen 5](#_Toc87801324)

[Grundlage für die nachfolgende Bewertung 5](#_Toc87801325)

[Kurze Beschreibung des Sachstandes 6](#_Toc87801326)

[Relevante offene Sicherheitsmaßnahmen 7](#_Toc87801327)

[Risikobewertung 9](#_Toc87801328)

[Maßnahmen zur Risikominimierung 10](#_Toc87801329)

[Benötigte interne Abteilungen 10](#_Toc87801330)

[Benötigte Dienstleister 10](#_Toc87801331)

Arbeitsblatt Beurteilung von Sicherheitsmeldungen

|  |  |
| --- | --- |
| Name: |  |
| Datum: |  |

Grundlage für die nachfolgende Bewertung

**Behandlung von Security Incidents und Reaktion auf Security-Advisories**

| Titel der Anforderung | Serviceklasse „Gold“ | Serviceklasse „Silber“ | Serviceklasse „Bronze“ |
| --- | --- | --- | --- |
| Verfügbarkeit (SLA/OLA) | 99,44 % pro Monat | 99,00 % pro Monat | 98,90 % pro Monat |
| Betriebszeit des Service | 24x7 | 24x7 | 24x7 |
| Maximale Ausfallzeit des kompletten Service | vier Stunden | sieben Stunden | 14 Stunden und 21 Minuten |
| Maßnahmen für die Erreichung einer Hochverfügbarkeit | Sind zu implementieren | Können implementiert werden | Sind nicht implementiert |
| Maximal tolerierbare Ausfälle des kompletten Service | zwei Ausfälle pro Jahr | fünf Ausfälle pro Jahr | 10 Ausfälle pro Jahr |
| Geo-redundante Rechenzentren | ja | Nein | Nein |
| Erfolgt die Bereitstellung über Cloud-Infrastrukturen | Ja | Teilweise | Teilweise |

|  |  |  |  |
| --- | --- | --- | --- |
| Kritikalitätsstufe | Serviceklasse „Gold“ | Serviceklasse „Silber“ | Serviceklasse „Bronze“ |
| CVSS Score: 7 - 10  Microsoft: Critical | Reaktionszeit (Annahme): 20 Min  Lösungszeit/Workaround: 10 Stunden | Reaktionszeit (Annahme): 20 Min  Lösungszeit/Workaround: 10 Stunden | Reaktionszeit (Annahme): 20 Min  Lösungszeit/Workaround: 10 Stunden |
| CVSS Score: 5 - 6  Microsoft: Moderate | Reaktionszeit (Annahme): 20 Min  Lösungszeit/Workaround: 24 Stunden | Reaktionszeit (Annahme): 20 Min  Lösungszeit/Workaround: 24 Stunden | Reaktionszeit (Annahme): 20 Min  Lösungszeit/Workaround: 24 Stunden |
| CVSS Score: < 5  Microsoft: Low | Reaktionszeit (Annahme): 20 Min  Lösungszeit/Workaround: mit dem nächsten Update (die Implementierung erfolgt im laufenden Betrieb) | Reaktionszeit (Annahme): 20 Min  Lösungszeit/Workaround: mit dem nächsten Update (die Implementierung erfolgt im nächsten Wartungsfenster) | Reaktionszeit (Annahme): 20 Min  Lösungszeit/Workaround: mit dem nächsten Update (die Implementierung erfolgt im nächsten Wartungsfenster) |

Die Kategorien für die Bewertung der Sicherheitsmeldung wurden bewusst einfach gehalten, um die Analyse überschaubar zu halten. Für die meisten IT-bezogenen Risiken und deren Ausnutzung ist eine genauere Bewertung in der Praxis ohnehin mit sehr großen Unsicherheiten verbunden. Die Bewertungsskalen sind:

| Bewertung von Eintrittswahrscheinlichkeiten | Bedeutung |
| --- | --- |
| auszuschließen/unwahrscheinlich | Eine Ausnutzung der Sicherheitslücke kann entweder ausgeschlossen werden oder ist so unwahrscheinlich, dass damit im Betrieb nicht gerechnet werden muss. |
| nicht auszuschließen/wahrscheinlich | Mit der Ausnutzung der Sicherheitslücke muss realistisch gerechnet werden. |

| Bewertung von Auswirkungen | Bedeutung |
| --- | --- |
| vernachlässigbar/gering | Durch die Ausnutzung der Sicherheitslücke entsteht kein Schaden, oder der resultierende Schaden ist so gering, dass er zusätzliche unverzügliche Aufwände für die Behandlung nicht rechtfertigt. |
| erheblich | Die Ausnutzung der Sicherheitslücke hat beträchtliche Auswirkungen und ist unmittelbar durch geeignete Maßnahmen zu begegnen. |

| Bewertung von Risiken | Bedeutung |
| --- | --- |
| tragbar | Das Risiko der Ausnutzung der Sicherheitslücke liegt im Rahmen der für einen IT-Betrieb unvermeidlichen Basisrisiken. Es erfordert keine Maßnahmen zur unverzüglichen Behandlung. |
| untragbar | Das Risiko der Ausnutzung der Sicherheitslücke geht über die für einen IT-Betrieb unvermeidlichen Basisrisiken hinaus und erfordert eine unverzügliche geeignete Behandlung.  Risiken werden als untragbar bewertet, wenn ihre Eintrittswahrscheinlichkeit „nicht auszuschließen/wahrscheinlich“ und ihre Auswirkungen „erheblich“ sind. |

Kurze Beschreibung des Sachstandes

|  |  |  |
| --- | --- | --- |
| ID der Sicherheitsmeldung: |  | |
| Inhalt der Sicherheitsmeldung: |  | |
| Einstufung der Sicherheitsmeldung: | CVSS Score: |  |
| Microsoft Score: | < Critical, Moderate, Low> |
| Schwachstellen nach Art: | Denial of Service: | <ja/nein> |
| Execute Code: | <ja/nein> |
| Overflow: | <ja/nein> |
| Bypass Something: | <ja/nein> |
| Gain Information: | <ja/nein> |
| Gain Privilege: | <ja/nein> |
| XSS: | <ja/nein> |
| Directory Traversal: | <ja/nein> |
| Sql Injection: | <ja/nein> |
| Memory Corruption: | <ja/nein> |
| Http Response Splitting: | <ja/nein> |
| CSRF: | <ja/nein> |
| File Inclusion: | <ja/nein> |
| Betroffene Prozesse/Services: |  | |
| Betroffene Assets: |  | |

Relevante offene Sicherheitsmaßnahmen

Aus der Prüfung der Anforderungen im IT-Grundschutz-Check resultierenden die folgenden offenen Grundschutz-Maßnahmen mit Bezug auf die zu beurteilende Sicherheitsmeldung.

Schicht ORP (Organisation und Personal)

| Nr. | Anforderung | Maßnahme |
| --- | --- | --- |
|  |  |  |

Schicht CON (Konzepte und Vorgehensweisen)

| Nr. | Anforderung | Maßnahme |
| --- | --- | --- |
|  |  |  |

Schicht OPS (Betrieb)

| Nr. | Anforderung | Maßnahme |
| --- | --- | --- |
|  |  |  |

Schicht DER (Detektion und Reaktion)

| Nr. | Anforderung | Maßnahme |
| --- | --- | --- |
|  |  |  |

Schicht APP (Anwendungen)

| Nr. | Anforderung | Maßnahme |
| --- | --- | --- |
|  |  |  |

Schicht SYS (IT-Systeme)

| Nr. | Anforderung | Maßnahme |
| --- | --- | --- |
|  |  |  |

Schicht IND (Industrielle IT)

| Nr. | Anforderung | Maßnahme |
| --- | --- | --- |
|  |  |  |

Schicht NET (Netze und Kommunikation)

| Nr. | Anforderung | Maßnahme |
| --- | --- | --- |
|  |  |  |

Die nachfolgenden Abschnitte beschreiben relevante Zusatzmaßnahmen nach den Schichten des BSI-IT-Grundschutz Kompendiums aus der bereits durchgeführten Risikoanalyse zusammen.

Schicht ORP (Organisation und Personal)

| Nr. | Beschreibung der zusätzlichen Maßnahme |
| --- | --- |
|  | **<Titel>**  <Beschreibung der Zusatzmaßnahme> |

Schicht CON (Konzepte und Vorgehensweisen)

| Nr. | Beschreibung der zusätzlichen Maßnahme |
| --- | --- |
|  | **<Titel>**  <Beschreibung der Zusatzmaßnahme> |

Schicht OPS (Betrieb)

| Nr. | Beschreibung der zusätzlichen Maßnahme |
| --- | --- |
|  | **<Titel>**  <Beschreibung der Zusatzmaßnahme> |

Schicht DER (Detektion und Reaktion)

| Nr. | Beschreibung der zusätzlichen Maßnahme |
| --- | --- |
|  | **<Titel>**  <Beschreibung der Zusatzmaßnahme> |

Schicht APP (Anwendungen)

| Nr. | Beschreibung der zusätzlichen Maßnahme |
| --- | --- |
|  | **<Titel>**  <Beschreibung der Zusatzmaßnahme> |

Schicht SYS (IT-Systeme)

| Nr. | Beschreibung der zusätzlichen Maßnahme |
| --- | --- |
|  | **<Titel>**  <Beschreibung der Zusatzmaßnahme> |

Schicht IND (Industrielle IT)

| Nr. | Beschreibung der zusätzlichen Maßnahme |
| --- | --- |
|  | **<Titel>**  <Beschreibung der Zusatzmaßnahme> |

Schicht NET (Netze und Kommunikation)

| Nr. | Beschreibung der zusätzlichen Maßnahme |
| --- | --- |
|  | **<Titel>**  <Beschreibung der Zusatzmaßnahme> |

Risikobewertung

|  |  |  |  |
| --- | --- | --- | --- |
| Vorhandene  Maßnahmen | <Aufzählung bzw. kurze Beschreibung der vorhandenen Maßnahmen> | | |
| Verbleibendes Risiko | Risikobewertung | Eintrittswahrscheinlichkeit | Auswirkungen |
| ◼ tragbar  ◼ untragbar | ◼ auszuschließen/ unwahrscheinlich  ◼ nicht auszuschließen/wahrscheinlich | ◼ vernachlässigbar/gering  ◼ erheblich |
| <kurze Risikobewertung> | | |

Maßnahmen zur Risikominimierung

| Nr. | Beschreibung der risikominimierenden Maßnahme |
| --- | --- |
| RM X.Y | **<Titel>**  <Beschreibung der Zusatzmaßnahme> |
| RM X.Y | **<Titel>**  <Beschreibung der Zusatzmaßnahme> |

Benötigte interne Abteilungen

| Abteilung | Kurzbeschreibung der benötigten Ressourcen und deren Skills |
| --- | --- |
|  |  |

Benötigte Dienstleister

| Dienstleister | Kurzbeschreibung der benötigten Ressourcen und deren Skills |
| --- | --- |
|  |  |