DGI® Deutsche Gesellschaft für Informationssicherheit AG

Bericht
zum Stand der Informationssicherheit

bei der Unternehmensname

für den Zeitraum
vom TT. MMMM JJJJ bis zum TT. MMMM JJJJ

Inhaltsverzeichnis

3 Vorwort

Dieser Bericht wird aufgrund der vereinbarten Aufgaben des ITSiBe aus der Benennung vom TT. MMMM JJJJ erstellt.

Der Bericht gibt die zur Kenntnis erlangten Sachverhalte zum Zeitpunkt der Erstellung wieder. Der Bericht ist durch die seitens der Unternehmensname (nachfolgend „Organisation“) benannten Personen an die Stakeholder, unter Wahrung der erforderlichen Vertraulichkeit, zu verteilen.

Die vertragliche Vereinbarung zur Benennung, namentlich durch Herrn / Frau Vorname Name, zum ITSiBe der Organisation führte zur Übernahme von Tätigkeiten, um das bestehende Niveau der Informationssicherheit der Organisation zum Zeitpunkt der Benennung festzustellen sowie das etablierte Niveau gemäß dem Stand der Technik und insbesondere unter Einhaltung der Anforderungen der auf die

Die vorgenannten Pflichten führen zudem zu einer erforderlichen Etablierung eines Risikomanagement- und Risikofrüherkennungssystems sowie zu der Einhaltung der Verkehrssicherungspflichten.

Ort, den TT. MMMM JJJJ

Vorname Name - ITSiBe der Organisation -

4 Management Summary

Die Motivation den Reifegrad des Informationssicherheitsmanagements der Organisation zu steigern wurde insbesondere durch die Projekte zur Einhaltung der eruierten Compliance-Anforderungen getrieben.

Die u. a. hieraus resultierende Benennung des ITSiBe führte insbesondere zu einem strukturierten Aufbau erforderlicher Prozess- und Dokumentenstrukturen, um das geforderte Sicherheitsniveau sukzessive zu erreichen sowie kontinuierlich zu verbessern.

Bei den Aktivitäten im Bereich der Informationssicherheit ist der Aufbau eines ISMS gemäß ISO 27001 hervorzuheben, welcher für eine spätere ISO 27001-Zertifizierung des Betriebs der IT-Infrastruktur und der IT-gestützten Anwendungen herangezogen werden kann.

Transparenz für die Umsetzung von Maßnahmen zur Sicherstellung des geforderten Informationssicherheitsniveaus und somit zu einer deutlich höheren Akzeptanz bei sämtlichen Stakeholdern.

Grundsätzlich kann der Organisation ein gutes Management der IT-Sicherheit bescheinigt werden, nichtsdestotrotz ist die Implementierung und Etablierung eines systematischen Vorgehens zur Aufrechterhaltung der Wirksamkeit umgesetzter Maßnahmen auch zukünftig zwingend nachzuhalten. Zudem sind Maßnahmen zur IT-Sicherheit oftmals nicht ausreichend, sofern die Einbindung in die gesamten Organisationsabläufe nicht sichergestellt ist. Der eigene Anspruch der Organisation, eine ganzheitliche Informationssicherheitsstrategie umzusetzen, kann in der Zukunft durch die kontinuierliche Verbesserung und Aufrechterhaltung der umgesetzten Maßnahmen sowie der fortlaufenden Anpassung und Neuentwicklung ergänzender Maßnahmen sicherlich zufriedenstellend erfüllt werden.

5 Aufnahme der Tätigkeit als ITSiBe

Im Rahmen eines zweitägigen Workshops wurden zahlreiche Interviews mit Stakeholdern bezüglich der angemessenen Wahrung insbesondere der Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität durchgeführt. Der Hintergrund der strukturierten Interviews war es Sicherheitsanforderungen in den einzelnen Teilbereichen der Organisation zu erfassen, mit dem Ziel Verbesserungspotentiale zur Steigerung des Managements der avisierten Informationssicherheit zu erkennen. Anschließend sollten angemessene Maßnahmen bestimmt und zur Umsetzung gebracht werden, die eine Fortentwicklung und Verbesserung des erreichten Informationssicherheitsniveaus sicherstellen.

Die Haupttätigkeit des ITSiBe lag in der Steuerung von Aktivitäten zum Aufbau eines ISMS und der Vermittlung vertiefender Kenntnisse zur Umsetzung eines Informationssicherheitsmanagementsystems, insbesondere an die beteiligten Stakeholder, sowie der Begleitung der Transition der IT-Infrastruktur zu

- der Kontrolle der Umsetzung der geforderten Maßnahmen
- der regelmäßigen Überwachung der IT-Infrastruktur
- der Überwachung der Entwicklung der Informationssicherheit
- der Anpassung des Informationssicherheitskonzepts an gewonnene Erkenntnisse
- der Untersuchung von Sicherheitsereignissen und -vorfällen
- der Koordinierung der Zusammenarbeit mit den für die Informationssicherheit relevanten Fachbereichen
- der regelmäßigen Erstellung des Berichts zum Stand der Informationssicherheit

unter Berücksichtigung der erforderlichen Mitwirkungspflichten der Organisation.

Die Risikoidentifikation in den einzelnen Bereichen, insbesondere im IT-Infrastruktur- und Clientbetrieb sowie dem IT-gestützten Anwendungsbetrieb, wurde durch die Führung persönlicher Interviews mit den Systemverantwortlichen sowie durch die Sichtung der hierfür explizit zur Verfügung gestellten Dokumente umgesetzt. Hierbei sind folgende Dokumente von hoher Prägnanz hervorzuheben, um Aussagen zur Risikoeinwirkung auf den ordnungsgemäßen Geschäftsbetrieb der Organisation treffen zu können

- sämtliche Dokumente zum Risikomanagement, insbesondere zur Risikoanalyse und -bewertung
- sämtliche relevanten Risikovermerke
- Dokumentation der IT-Strategie
- Dokumentation der Ableitung und Operationalisierung der IT-Strategie
- Dokumentation der Informationssicherheitsstrategie (Informationssicherheitsleitlinie)
- Compliance-Berichte
- Dokumente der Ordnungsmäßigkeitsprüfung

weiterverfolgt werden.

Die Erstellung der Informationssicherheitsleitlinie, unter Einbeziehung der Geschäftsstrategie und der Geschäftsziele sowie der IT-Strategie der Organisation, wurde im Berichtszeitraum abgeschlossen.

Die mit dem Bereich IT und dem Bereich Informationssicherheit final abgestimmte Informationssicherheitsleitlinie liegt der Geschäftsführung als Vorlage und zur Freigabe vor.

Die effiziente Erstellung von Dokumentationen zum Notfallmanagement wurde aufgrund der Transition der IT-Infrastruktur zum Dienstleister zurückgestellt, da die operativen Prozesse und die erforderlichen Handlungsanweisungen erst mit Abschluss der Transition, beziehungsweise der Aufnahme und

Überwachung des normalisierten Betriebs der IT-gestützten Geschäftsprozesse der Organisation, eindeutig beschreibbar sein werden.

Die Ausarbeitung von Dokumentationen für die Planung, Steuerung und Kontrolle der erforderlichen Prozesse zur Umsetzung des avisierten Informationssicherheitsniveaus hat im Berichtszeitraum einen deutlichen Reifegewinn erfahren. Die Finalisierung sowie Freigabe der Dokumentationen sollte nach Abschluss des Transitionsprojekts mit dem Dienstleister erfolgen, um ein effizientes und effektives Vorgehen durchzusetzen. Des Weiteren sollten die Änderungen sowie Neuerstellungen der Dokumentationen mit dem transferierten IT-Infrastrukturbetrieb und den Anforderungen einer beabsichtigten ISO 27001-Zertifizierung in Einklang gebracht werden.

Die im Berichtszeitraum erstellten Dokumentationen sind im Kapitel "Anlage Dokumentenverzeichnis" aufgeführt.

dem Abschluss angemessener Servicevereinbarungen, insbesondere mit den relevanten Dienstleistern, sichergestellt.

Das Management von Informationssicherheitsvorfällen des IT-Infrastrukturbetriebs mit den relevanten Dienstleistern wurde durch das Konzept IT-Servicemanagement geregelt.