VA Notfallmanagement im Rahmen der IT-Sicherheitsnormen (z.B. Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI))

Übersicht

Der Art. 32 DSGVO/§ 64 BDSG regelt technische und organisatorische Maßnahmen (TOM) für kleine und mittlere Unternehmen (KMU) zum Schutz vor Schadensfällen in der IT-Anwendung.

Referenz: Auszug Art. 32 der Datenschutz-Grundverordnung (DSGVO):

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter ***geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.***

Ziel und Zweck

Die Verfahrensanweisung hat das Ziel, die Abläufe und allgemeinen Regelungen zum Notfallmanagement in der IT-Sicherheit in strukturierten Prozessen und Verfahren transparent umzusetzen und gut verständlich darzustellen. Ziel dieser Beschreibung ist die Vereinheitlichung der Abläufe und die Sicherstellung des Prozesses, der geregelt wird und die Gewährleistung der Vollständigkeit sowie der geplanten Ergebnisqualität.

Anwendungsbereich

Diese Anweisung gilt für alle Anwendungen in betrieblichen Prozessen mit Einsatz von Informationstechnik inklusive mobiler Endgeräte wie Smartphones, Tabletcomputer und Laptops.

Verantwortung

Verantwortlich für die einzelnen Segmente des Verfahrens sind dazu beauftragte Personen, insbesondere:

- Geschäftsleitung/Mitglieder der Leitung
- Informationssicherheitsbeauftragte (ISB)
- Datenschutzbeauftragte (DSB) und Datenschutzkoordinierende (DSK)
- Externe Dienstleistende, soweit rechtlich geregelt (externe Datenschutzbeauftragte (DSB))

Die individuellen Verantwortungsbereiche sind in Protokollen, falls vorgesehen, zu dokumentieren.

Prozesse

Zum IT-Notfallmanagement gehört im ersten Schritt die Definition und Beschreibung eines IT-Notfalls. Diese Festlegungen hängen vom einzelnen Betrieb und dem Computerisierungsgrad ab. So kann definiert werden, dass ein Notfall dann vorliegt, wenn für die operativen Abläufe wichtige Arbeitsplätze für einen längeren Zeitraum (z.B. länger als 60 Minuten) ausfallen. Für diesen Fall müssen Notfallpläne vorliegen, z.B. für unterbrochene oder abgebrochene Untersuchungen oder Therapien.

Konkrete Fragestellung: Wurde überprüft, ob es sich um einen tatsächlichen IT-Notfall handelt, erfolgt die Meldung an den oder die IT-Verantwortliche*n? Dies erfolgt im Regelfall über ein Mobiltelefon, das immer unabhängig vom Computer- und Stromnetzwerk funktionieren muss.

Für die praktische Nothilfe muss ein Aushang vorhanden sein, der den oder die IT-Notfallbeauftragte*n und seine/ihre Telefonnummer enthält. Weiterhin müssen Verfahrensanweisungen oder interne Regelungen im Rahmen des Qualitätsmanagements vorliegen.

Danach sind die verschiedenen IT-Notfälle zu klassifizieren:

- Ausfall eines einzelnen IT-Arbeitsplatzes
- Ausfall aller IT-Arbeitsplätze einer Abteilung
- Ausfall des gesamten IT-Netzwerks

Im Rahmen des Qualitätsmanagements gibt es Checklisten und Verfahrensanweisungen/interne Regelungen für die möglichen Schweregrade eines IT-Notfalls.

Aktualisierung: nach 12 Monaten

Mitgeltende Dokumente:

- Bundesdatenschutzgesetz **(BDSG) Auszug § 64**
- Datenschutz-Grundverordnung **(DSGVO) Auszug Art. 32**
- Normen für IT-Sicherheit nach BSI Grundschutz
- ISMS Rahmenbedingungen nach VdS 10000 Standard

Leitlinie zur IT-Sicherheit im Betrieb/Unternehmen