Inhalt

Zweck und Anwendungsbereich

Der Chief Information Security Officier (CISO) ist die Hauptverantwortliche Person für dieses Dokument.
Das Dokument wird dazu benötigt, um im Falle eines Ausfalles eine Strategie zur Behebung dieses Ausfalles zu haben. Hierfür wird ein Plan-Do-Check-Act-Zyklus (PDCA-Zyklus) für die Sicherung der technischen- organisatorischen Maßnahmen verwendet. Hierbei handelt es um ein Dokument, dass laut dem Traffic Light Protcoll der Farbe „Amber“ unterstellt ist. Dementsprechend wird das Dokument nur innerhalb der Abteilung und nur an Personen, für die diese Wissens essenziell ist, weitergegeben werden. Das Dokument bezieht sich hierbei auf die rechtlichen Grundlagen des österreichischen Gesetzes. Wobei man sich hierbei besonders an Kapitel elf und zwölf des österreichischen Sicherheitshandbuch halten kann. Die Patientendaten werden mit der Datenschutzgrundverordnung, der Netz- Informationssystemsicherheitsgesetz und dem Gesundheitstelematikgesetz geschützt und nach diesen Gesetzen wird gehandelt.

Geltungsbereich

Das Dokument ist hierbei für die Mitarbeiter und Mitarbeiterinnen der Klinik-Wien-6-Tage wichtig und wird deswegen mit der Farbe „Amber“ des Traffic Light Protocol behandelt, da es für außenstehende Personen, die nicht in der Klinik arbeiten irrelevant ist.

Grundlagen

Da die Klinik-Wien-6-Tage mit Patientendaten arbeiten und diese Daten geschützt werden müssen, wird nach der EU-Datenschutz Grundverordnung (DSGVO) und nachdem Netz- und Informationssystemsicherheitsgesetzt (NISG) gearbeitet und die hochsensiblen Daten der Patienten geschützt werden. Ebenso kommt es innerhalb der Klinik zu unterschiedlichen Vorgangsweisen der Ausfallsicherheit bezüglich der Mitarbeiter. Nicht jeder Mitarbeiter hat zu jedem Bereich Zugang, weshalb Rollen unterschieden werden müssen.

Einmal jährlich wird das Dokument von einem Juristen überprüft und Anpassung nach den aktuellen Gesetzen durchgeführt. Der CSIO ist für die laufende Kontrollierung des Dokumenten und die Kontrolle des Dokumentes zuständig. Die Veröffentlichung und die Endkontrolle vor der Veröffentlichung des Dokumentes findet durch das Gremium statt.

Ablauf für Ausfallssicherheitsrichtlinie

Das IT-Netz sollte Bereich aufgespalten werden. Notwendige Kernprozesse, Prozesse, die für den Betrieb der Kernprozesse notwendig sind und sonstige Prozesse in der Klinik.
Zuerst muss überlegt werden, welche Tätigkeiten und Prozesse in der Klinik essenziell sind, danach wird überlegt, welche Risiken es für diese Prozesse gibt und warum es zu Ausfällen kommen kann. Es sollte nicht nur zu einer Unterscheidung der Prozesse in der gesamten Klinik kommen. Ebenfalls sollten die einzelnen Abteilungen analysiert werden und die Kernprozesse herausgearbeitet werden, die auch in einem Notfall direkt wieder anwendbar sein müssen.
Während einem Ausfall sollte ein Krisenteam, dass vor einem eintretenden Notfall definiert wird, Anweisungen erteilen. Diese Anweisungen müssen vom Personal befolgt werden, um einen trotz Ausfall möglichst geregelten Klinikablauf beizubehalten.
Nach einem Ausfall von IT-Geräten muss es zu einer Datenwiederherstellung kommen beziehungsweise die Daten, die während des Ausfalles entstanden sind, müssen in die IT eingespielt werden. Falls es zu einem Schaden der Technik kommt, muss dieser umgehend ersetzt oder repariert werden.
Die Überprüfung der Ausfallssicherheitsrichtlinie sollte alle vier Monate mittels einem erstellten Protokoll überprüft werden, außer es kommt zu einem Problem in einer nahestehenden Klinik, dann sollte die Ausfallssicherheitsrichtlinie früher überprüft werden. Falls während der Überprüfung weitere Geräte festgestellte werden, die für den Weiterbetrieb in einer Ausfallsicherheit von Nöten sind, müssen diese in das Ausfallkonzept hineingearbeitet werden.
Bei Problemen bei der Überprüfung muss früher die Ausfallssicherheitsrichlinie überprüft werden und eine Anpassung der Ausfallssicherheitsrichtlinie erfolgen.

- Erstellung eines Gremiums
  - Verantwortlicher für DSGVO
  - CISO
  - IT-Leiter
  - Leiter der unterschiedlichen Abteilungen der Klinik
  - Verantwortlicher für medizinische Geräte
- Teams bilden
- Kernprozesse herausfiltern
- Sicherheitskonzept erstellen
- Kernprozesse schützen vor Ausfall
- Regelmäßige Überprüfungen, ob Ausfallsicherheitskonzept passt

Falls es zu einem Ausfall außerhalb der Geschäftszeiten der Klinik kommt, werden diese Probleme erst mit erneuten Dienstbeginn behoben, da die Klinik nicht dauerhaft benötigt wird und nicht für Notfälle gedacht ist und ein kurzfristiger Ausfall außerhalb der Öffnungszeiten keine Menschenleben fordern würde.

Sollte es aber zu einem Diebstahl von Patientendaten kommen, muss dieser Notfall auch außerhalb der Geschäftszeiten an die Datenschutzbehörde und an das Netz- und Informationssystemsicheheitsbehörde gemeldet werden. Diese Meldung muss innerhalb der ersten drei Stunden, besser früher, erfolgen.

IKT-Notfallstrategie

Für den Aufbau einer Notfallstrategie kann auf das österreichische Sicherheitshandbuch, Kapitel 11 und 12 „physische und umgebungsbezogene Sicherheit“ beziehungsweise Sicherheitsmanagement im Betrieb“ verwiesen werden. Hierbei handelt es bei Kapitel elf um einen Schaden von außen durch Unachtsamkeiten oder andere Umwelteinflüsse und bei Kapitel zwölf um Sicherheitsmanagement im Betrieb vor allem im Fokus die Etablierung eines IT-Sicherheitskonzepts. Zuerst sollte es zu einer Dokumentation aller verwendeten Geräte und Software kommen, damit diese im Notfall übersichtlich sind und auch bei Überprüfungen klar ist, welche Geräte beziehungsweise Software verwendet wird. Weiteres muss es zu Schutzmaßnahmen gegen Schadsoftware und Schadfunktionen kommen, damit die Ausfallwahrscheinlichkeit minimiert wird und es zu weniger Notsituation im laufenden Betrieb kommen kann. Schadsoftware kann mittels einer Firewall schon vor dem Eintritten in die IT der Klinik herausgefiltert werden. Ebenso muss es zu einer Schulung des Klinikpersonals kommen, damit diese Phisingemails mit möglichen Viren erkennen, löschen und an die IT weitermelden, damit es zu keinem Virus in der IT im Spital kommt, da dadurch Geräte des Kernprozessen langfristig ausfallen können
Um einen Ausfall von IKT-Komponenten zu kompensieren oder zu vermeiden, sollte es Redundanzen geben, um bei etwaigen Problemen einzelner IKT-Geräte einen Ersatz schon in der Klinik zu haben. Fall es zu einem Brandfall kommt muss es für die gesamte Klinik einen Plan geben, der nur an die jeweiligen Umgebungen angepasst ist, ebenso muss es in speziellen Räume feuerdämmende Maßnahmen geben, um das Leben der mitarbeitenden oder behandelten Personen nicht zu gefährden.

IKT-Notfallversorgung

Für die wichtige IT sollte es, wie für wichtige medizinische Geräte eine Notstromversorgung geben, am besten ist diese Notstromversorgung eine Unterbrechungsfreie Stromversorgung, damit in Kernprozessen ohne Probleme

weitergearbeitet werden kann. Bei einem Ausfall von einzelnen Geräten müssen in der Klinik schon Ersatzgeräte sein. Ebenfalls von Vorteil ist es, wenn das gesamte Personal die gleiche Ausstattung an IT-Geräten hat, dadurch können Geräte an wichtigeres Personal in der Klinik weitergegeben werden. Falls es zu einem Ausfall der gesamten IT in der Klinik kommt

Meldeprozesse nach NISG und DSVGO

Nach einem Angriff auf das Spital, speziell auf die IT muss innerhalb von drei Stunden eine Meldung an das NISG geschickt werden. Dabei sollten alle Probleme protokolliert weitergegeben werden und die betroffenen Abteilungen zusammenarbeiten und gemeinsam hierfür ein Protokoll erstellen.
Nach einem Angriff muss nicht nur die NISG gemeldet werden, sondern auch an die DSVGO. Hierbei gilt bei einem Datenverlust von Patientendaten eine direkte Meldungen, ansonsten hat der Spital bis zu 72 Stunden Zeit, dennoch sollte die Meldung unverzüglich erfolgen.
Für die Übermittlung und Sammlung der Daten ist ein dafür im Vorfeld gegründetes Team zuständig.