Inhalt

1 Zweck und Anwendungsbereich

Dieses Dokument definiert, wie die Datenschutz- und Informationssicherheit und die Ausfallsicherheit in der Tagesklinik „Magareten-Tagesklinik“ umgesetzt werden muss. Dieses Dokument gilt in der gesamten Unternehmensstruktur und muss ohne Ausnahme befolgt werden. Das Dokument basiert auf die rechtlichen Gegebenheiten des österreichischen Gesetzesrahmen.

2 Datenschutz- und Informationssicherheitskozept

2.1 Organisatorische Maßnahmen

Für den Prozess wird ein Team zusammengestellt, das sich aus 5 Personen zusammenstellt. Das Team stellt sich aus dem CISO, 3 Fachkräfte der ISMED-Organisation und eine Fachkraft von der Tagesklinik zusammen. Es ist nötig, dass sich das Team bei Normalbetrieb jede zweite Woche trifft und mögliche Bedrohungen, Gefährdungen erkennt und folgend Maßnahmen plant und demnach diese auch in der Tagesklinik umsetzt. Diese Änderungen an der Sicherheitsrichtlinie werden schriftlich festgehalten, damit die gesamt IT-Organisation informiert wurde. Die Sicherheitsrichtlinie, um die Infrastruktur des Systems bestmöglich zu sichern, wird vom IT-Team geplant. Dabei wird der Datenschutz der personenbezogenen Daten (DSGVO) und das NISG vollständig beachtet. Um das Niveau der Infrastruktur aufrecht zu erhalten, wird die CIA-Triade verwendet. Der IT-Leiter (CISO) ist der Verantwortliche und trägt die Verantwortung, dass die Planung ordnungsgemäß abläuft.

2.2 Technische Maßnahmen

Da es technisch möglich ist, werden jegliche Daten, die in der Datenbank der Tagesklinik gespeichert werden, verschlüsselt abgespeichert. Ärzte und Pflegepersonal bekommen eine Chipkarte, die eine Zutrittskontrolle schafft. Demnach können Patienten nicht ohne Personal in die Untersuchungs- und Behandlungszimmer. Mit der Chipkarte des Oberarztes ist es auch möglich die Zutrittskontrolle mit Chipkarte manuell auszustellen. Dies ist bei einem Notfall nützlich. Die Stand-PC im Untersuchungsbereich und im Behandlungsbereich sind passwortgeschützt, die nur einmal am Anfang des Betriebes entsperrt werden müssen. Die PCs im Wartebereich und in der Anmeldung werden nach 10 Minuten Inaktivität gesperrt, da diese keinen Zutrittskontrolle für Patienten bietet. Für Mitarbeiter, die von Zuhause arbeiten, ist es nur möglich, mit VPN zu einem Server zu verbinden. Dabei ist der Laptop/der PC nur ein Terminal und die tatsächlichen Daten befinden sich nicht am lokalen PC. Dadurch ist es nicht möglich, Daten abzugreifen.

3 Ausfallsicherheitskonzept

3.1 Organisatorische Maßnahmen

Die Service der Tageskliniken werden nach Priorität nach Gold, Silber, Bronze Kriterien eingestuft. Dabei haben die Service, die Gold eingestuft werden die höchste Priorität. Bei einer Netzwerkauslastung werden die Service (z.B. Anmeldungen) so weit hinuntergefahren, dass die Gold-Service ungehindert weiter arbeiten können. Bei einem Notfall muss ein Notfallteam eingerufen werden. Dieses wird von dem Notfallteamleiter geleitet, der in der Zeitspanne des Notfall die volle Macht hat, um den Normalbetrieb wieder herzustellen. Es ist definiert, dass ein Störfall innerhalb 3h Stunden Die Daten müssen auch bei Ausfall gespeichert sein. Bei einem Verdacht auf eine Data-Bridge muss dies laut der Datenschutzgrundverordnung innerhalb 72h gemeldet werden. Bei einer Ströung eines wesentlichen Dienstes muss dies, wenn nicht innerhalb von 3h der Normalbetrieb einkehrt, auch gemeldet werden. Das Team muss außerdem ein Störfallkatalog bereitstellen, der den Mitarbeitern (Ärzten, Krankenpfleger, etc.) informiert, was bei einem akuten Störfall zu tun ist. Bei einem Notfall, ein nicht bekannte Gefährdung oder Bedrohung, die für die Organisation unbekannt ist, muss ein Notfallplan bereitstehen. Siehe Punkt 3

3.2 Technische Maßnahmen

Um die Datensicherheit bei einem Ausfall des Rechenräume zu gewährleisten, werden die Daten auch parallel in einer Cloud-Lösung, die die DSGVO beachtet gespeichert, sodass die Verfügbarkeit der Daten jederzeit gegeben ist. Die Behandlungs- und Untersuchungsräume sind mit Notfall-Knöpfe ausgerüstet, die das Notfallteam sofort per Handy-App alarmiert. Bei einem Ausfall eines PC müssen Ersatzgeräte zur Verfügung stehen, die innerhalb von 30 Minuten fertig konfiguriert wurde. Außerdem gibt ein Diesel-Aggregat, der die Stromversorgung für die wesentlichen Service (Dienste mit der höchsten Priorität) bei einem Stromausfall übernimmt. Dieser muss mindestens für 2 Stunden halten. In dieser Zeit wird der Betrieb auf ein Minimum reduziert.