Begonnen am	Montag, 27. Mai 2019, 15:31
Status	Beendet
Beendet am	Montag, 27. Mai 2019, 16:12
Verbrauchte Zeit	41 Minuten 13 Sekunden
Bewertung	**94,00** von 100,00
Feedback	Sehr gut (1)

Frage **1**

Vollständig

Erreichte Punkte 32,00 von 32,00

Sie haben in den letzten Wochen über das "Netz- und Informationssystemsicherheitsgesetzes (NISG)" im Gesundheitswesen gehört. Ein wichtiger Teil sind "technische und organisatorische Maßnahmen (TOMs)", die auch im Art. 32 der DSGVO gefordert werden.

Ein wichtiger Teil ist die Verfügbarkeit des Netzwerkes im Spital, da immer mehr Tätigkeiten bei der Behandlung von Personen im Spital von Informations- und Kommunikationstechnik (IKT) abhängen.

In der SPENGERKLINIK werden die kritischen Prozesse in einem Workshop des Projektteams ausgewählt.

Organisations-einheit	*Prozess*	*Kritikalität (Ja, Nein)*	*Begründung*
Intensivstation	Aufnahme	Nein	Verzögerungen können sich erst nach langer Zeit gravierend auf die Gesundheit eines Patienten auswirken.
	Behandlung	Nein	Verzögerungen können sich erst nach langer Zeit gravierend auf die Gesundheit eines Patienten auswirken.
	Verlegung/Entlassung	Ja	Verzögerungen im Rahmen des festgelegten Kriteriums wirken sich kritisch auf die Gesundheit eines Patienten aus.
Radiologie	Radiologische Diagnostik	Nein	Verzögerungen können sich erst nach langer Zeit gravierend auf die Gesundheit eines Patienten auswirken.
Chirurgische Station	Stationäre Behandlung	Nein	Verzögerungen können sich erst nach langer Zeit gravierend auf die Gesundheit eines Patienten auswirken.
Notaufnahme	Notaufnahme	Nein	Verzögerungen können sich erst nach langer Zeit gravierend auf die Gesundheit eines Patienten auswirken.
Küche	Verpflegung	Ja	Auch längere Ausfälle können nicht überbrückt werden, da im Notfall erforderliche Verpflegung extern nicht angeliefert werden kann.

Tabelle 1: Beispiel für die Bewertung der Prozesskritikalität in der SPENGERKLINIK

Beschreiben Sie mit mindesten 8 Sätzen:

*a) Warum diese Richtlinie **RICHTIG** ist oder **FALSCH** ist.*
b) Welche Maßnahmen leiten Sie bei der IKT-Unterstützung für diese Prozesse ab?

Sie leiten den Punkt a) mit den Worten ein: Diese Richtlinie ist (FALSCH / RICHTIG), weil ...
Sie leiten den Punkt b) mit den Worten ein: Folgende Maßnahmen sind für die Prozesse bei der IKT-Unterstützung zu berücksichtigen: ...

BEGRÜNDEN SIE IHRE ENTSCHEIDUNG *mit mind. 8 Stätze!*

Die Richtlinie ist für mich persönlich zum größten Teil Falsch. Die Begründung folgt in den nächsten Absätzen.

Der Prozess "Aufnahme" müsste, meiner Meinung nach als "kritisch" eingestuft werden. Wenn ein Patient bei der Aufnahme nicht rechtzeitig im Spital aufgenommen wurde, so kann er, im Ernstfall, auch nicht richtig behandelt werden. Zeit und Verzögerungen können bei Fällen, bei denen der Patient schnelle Hilfe benötigen, großen Schaden anrichten. Ebenfalls könnte dort auch die Priorität nicht richtig weiter gegeben werden, wenn das System große (lange) Verzögerungen hat.

Der Prozess "Behandlung" sollte meiner Meinung nach ebenfalls als "Kritisch" angesehen werden. Wenn ein Patient zu lange auf seine Behandlung warten muss, obwohl er diese viel früher benötigt, kann dieses großen körperlichen Schaden am Patienten als Folge haben. Beispielsweise bei einem allergischen Effekt, Atemnot, Wunden. Die Informationen zur Behandlung sollten schnellst Möglich weitergegeben werden.

Bei der "Verlegung/Entlassung" kann ich nur teils zustimmen, nachdem die Verlegung als kritisch angesehen werden kann. Wenn ein Patient schnellst Möglich verlegt werden muss, um keine körperlichen Folgeschäden zu haben, dann sollte die Verlegung schnellst Möglich passieren. Anders ist es bei der Entlassung. Da kann es auch als "kritisch" angesehen werden, nachdem bei manchen Spitäler ein Platzmangel (Bettenmangel) herrscht. So kann es schon relevant sein, möglichst viele Plätze freizuhalten. Die Entlassung kann jedoch keine medizinischen Folgen im Normalfall haben.

Radiologische Diagnostik sollte als "Kritisch" angesehen werden, nachdem die Radiologie zur schnellen Aufklärung von relevanten medizinischen Notfällen von Nöten ist, um den Patient, auch in Lebensbedrohlichen Situationen schnellst möglich helfen zu können.

Stationäre Behandlung sollte auch als kritisch anzusehen sein, zumindest die Teile, die Folgeschäden bei dem Patienten auslösen können (oder Lebensgefährlich sind). Innerhalb der Chirurgie sollten jedoch alle medizinischen Geräte auch bei Notfällen, beispielsweise Stromausfällen voll Funktionsfähig sein, zumindest die wichtigsten Funktionalität sollten auch da funktionieren.

Die Notaufnahme sollte ebenfalls als kritisch zu sehen sein, nachdem dort viele, ernste Notfälle sein können. Lebensgefährlich Verletze/Kranke Patienten landen dort. Viele Patienten von Unfällen werden auch dort eingeliefert.

Die Verpflegung in der Küche ist als relativ kritisch anzusehen. Patienten, die gewisse Nährstoffe bekommen, sollte als kritisch angesehen werden, und Patienten, die nicht auf der Sekunde Essen benötigen als nicht kritisch. Auch sollte die Zeit des Ausfalles berücksichtigt werden.

Eine extra Unterteilung un vielen Fällen wäre von nötig.

Folgende Punkte, sind aufgrund der vorherigen Absätze zu berücksichtigen:

1. Bestimmte Punkte sollten extra unterteilt werden
2. Die Tabelle stimmt nur in gewissen Punkten, weil es auf die Situation und Ansichten ankommt.
3. Es sollte immer Abgewogen werden, ob Menschenleben in Gefahr ist oder nicht, wenn man einen Punkt als "kritisch" oder "nicht kritisch" einstuft
4. Ebenfalls sollten Punkte auch eingestuft werden, ob Folgeschäden am Patienten enstehen können.

Kommentar:

IHRE Begründung ist schlüssig und hat folgende Aspekte berücksichtigt:

Diese Richtlinie ist FALSCH, weil die Kritikalität in der Tabelle 1 FALSCH bewertet wurde.

Die RICHTIGE Bewertung ist

Folgende Maßnahmen sind für die Prozesse bei der IKT-Unterstützung zu berücksichtigen:

Ein wichtiger Faktor der IKT-Unterstützung ist die Betrachtung der Bedrohung der VERFÜGBARKEIT, INTEGRITÄT und VERTRAULICHKEIT pro Prozess. Die in der Tabelle angeführte Kritikalität und Abhängigkeit führt zur Priorisierung.

Die Priorisierung der VERFÜGBARKEIT und INTIGRITÄT vor der VERTRAULICHKEIT im Spital ist wichtig, weil, die MEDIZINISCHE ENTSCHEIDUNG von der VERFÜGBARKEIT und der INTIGRITÄT der DATEN ABHÄNGT. Die VERFÜGBARKEIT kann durch eine REDUNDANZ und die INTIGRITÄT durch Plausibilitätsprüfung und/oder eine SIGNATUR erhöht werden. Die VERTRAULICHKEIT gilt natürlich immer, außer wenn dadurch das Leben eines Menschen gefährdet ist.

„SECURITY by Design & Default“ (Verfügbarkeit + Integrität der CIA-Triade) und „PRIVACY by Design & Default“ (Vertraulichkeit der CIA-Triade) sind umgesetzt durch

- ein Information Security Management System (ISMS) ist vorhanden
- ein Datenschutz Management System (DSMS) ist vorhanden

Frage **2**

Vollständig

Erreichte Punkte 34,00 von 34,00

Sie haben in den letzten Wochen über das "Netz- und Informationssystemsicherheitsgesetzes (NISG)" im Gesundheitswesen gehört. Ein wichtiger Teil sind "technische und organisatorische Maßnahmen (TOMs)", die auch im Art. 32 der DSGVO gefordert werden.

Ein wichtiger Teil ist die Verfügbarkeit des Netzwerkes im Spital, da immer mehr Tätigkeiten bei der Behandlung von Personen im Spital von Informations- und Kommunikationstechnik (IKT) abhängen.

Richtlinie für RISIKO-ANALYSE:

Für die Definition der **IKT-Schutzziele** können die drei in der Informationssicherheit üblichen Grundwerte **Verfügbarkeit**, **Integrität** und **Vertraulichkeit** herangezogen werden. Dem übergeordneten Schutzziel der Einrichtung "SPITAL" entsprechend werden diese drei Grundwerte allerdings im Rahmen der IKT-Risikoanalyse nicht als gleichrangig betrachtet, sondern sind untereinander priorisiert.

An oberster Stelle steht die Sicherung der Verfügbarkeit von Anwendungen und IKT-Systemen sowie der Verfügbarkeit und Integrität der mit diesen verknüpften Informationen.

Das Schutzziel der Vertraulichkeit wird zwar ebenfalls in die Betrachtung einbezogen, allerdings unter dem Blickwinkel der Folgen betrachtet, die sich aus einer Verletzung dieses Schutzziels für die Verfügbarkeit und Integrität ergeben können.

Beschreiben Sie mit mindesten 8 Sätzen:

*a) Warum diese Richtlinie **RICHTIG** ist oder **FALSCH** ist.*

Sie leiten den Punkt a) mit den Worten ein: Diese Richtlinie ist (FALSCH / RICHTIG), weil ...

BEGRÜNDEN SIE IHRE ENTSCHEIDUNG *mit mind. 8 Stätze!*

Diese Richtlinie ist zum Teil Richtig. Natürlich ist es relevant, dass IKT Systeme dauerhaft lauffähig sind, jedoch sollte es auch nicht Möglich sein Daten abzufangen (Daten zu klauen), wenn einmal Teile des Systems nicht in Betrieb sind. Auch sollte dafür gesorgt werden, dass Daten soweit noch gespeichert werden können, dass sie bei einem Ausfall nicht verloren gehen. Das heißt jedoch nicht, dass diese Daten so gespeichert werden, dass sie abgegriffen werden können. Berechtigungen sollten erteilt werden, sodass wirklich nur die Personen, die berechtigt sind worauf zu zu greifen, dass machen können.

Beispielsweise: Eine Sicherheitseinrichtung im Spital fällt aus. Wären keine anderen Sicherungsmaßnahmen vorhanden, dass keine Datensätze manipuliert oder abgegriffen werden können, könnte viel beeinflusst werden. Wesentliche Gerätschaften, die beispielsweise der Patient benötigt, um zu Überleben, könnten abgeschalten, oder so manipuliert werden, dass der Patient Folgeschäden erleidet, wenn nicht sogar in eine lebensbedrohliche Situation versetzt wird. Ebenfalls könnten private Patientendaten gestohlen werden, welche auch von den Versicherungen verwertet werden können oder Patienten zu schaden. Deswegen sollte es mehrer Sicherheitssysteme geben, die sicherstellen, dass nur berechtigtes Person, in jeder Situation, bestimmte Daten bearbeiten, abrufen und löschen können (Daten beeinflussen können).

Kommentar:

IHRE Begründung ist schlüssig und hat folgende Aspekte berücksichtigt:

Diese Richtlinie ist RICHTIG und/oder FALSCH, weil im Gesundheitswesen der Schutz der Person an 1. Stelle gestellt wird. Es muss pro Prozess entschieden werden, ob die Bedrohung der VERFÜGBARKEIT und der INTIGRITÄT gleich oder eine der beiden Bedrohung wichtig ist. Es gilt dabei immer SAFETY vor SECURITY.

„SAFETY“ bedeutet den Schutz der Umgebung vor einem Objekt.

„SECURITY“ stellt den Schutz des Objektes vor der Umgebung sicher, etwa durch das Verhindern des Eindringens unbefugter Software (Viren-Schutz).

Die Priorisierung der VERFÜGBARKEIT und INTIGRITÄT vor der VERTRAULICHKEIT im Spital ist wichtig, weil, die MEDIZINISCHE ENTSCHEIDUNG von der VERFÜGBARKEIT und der INTIGRITÄT der DATEN ABHÄNGT. Die VERFÜGBARKEIT kann durch eine REDUNDANZ und die INTIGRITÄT durch Plausibilitätsprüfung und/oder eine SIGNATUR erhöht werden. Die VERTRAULICHKEIT gilt natürlich immer, außer wenn dadurch das Leben eines Menschen gefährdet ist.

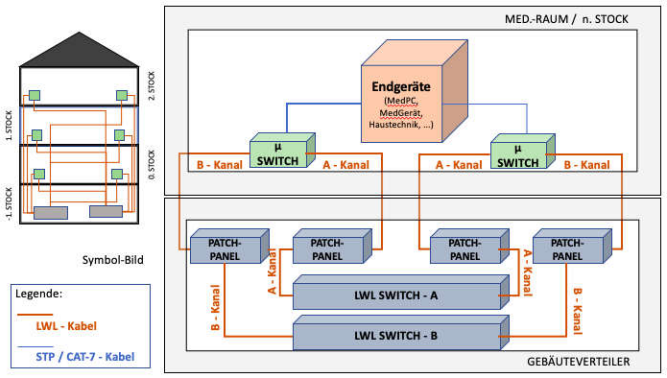
Frage **3**

Vollständig

Erreichte Punkte 28,00 von 34,00

Sie haben in den letzten Wochen über das "Netz- und Informationssystemsicherheitsgesetzes (NISG)" im Gesundheitswesen gehört. Ein wichtiger Teil sind "technische und organisatorische Maßnahmen (TOMs)", die auch im Art. 32 der DSGVO gefordert werden.

Ein wichtiger Teil ist die Verfügbarkeit des Netzwerkes im Spital, da immer mehr Tätigkeiten bei der Behandlung von Personen im Spital von Informations- und Kommunikationstechnik (IKT) abhängen.



***Für den LABOR-Bereich (MED.-Raum) gibt es daher eine Netzwerk-Topologie-Richtlinie**, die beim Aufbau umgesetzt werden muss (siehe Symbol-Bild).*

Weiters sind folgende Punkte bei den elektrischen Anschlüssen im Gebäudeverteiler-Raum und den "µ SWITCH" zu beachten:

Stromkreise:
Pro Netzwerkschrank sind zwei unabhängige über jeweils eigene FI-LS geführte Stromkreise herzustellen, wobei einer der beiden über das Normalnetz der Anstalt und der zweite Stromkreis über das Notstromnetz zu führen ist.

Potentialausgleich:
Alle leitenden Teile des Schrankes sind untereinander zu verbinden (an den im Schrank vorbereiteten Potentialausgleichsklemmen) und gesammelt an die nächste Sammelerdungsschiene zu führen.

Beschreiben Sie mit mindesten 8 Sätzen:

*a) Warum diese Richtlinie **RICHTIG** ist oder **FALSCH** ist.*
b) Welche(n) Punkt(e) Sie noch beachten würden.

Sie leiten den Punkt a) mit den Worten ein: Diese Richtlinie ist (FALSCH / RICHTIG), weil ...
Sie leiten den Punkt b) mit den Worten ein: Ich würde folgende(n) Punkt(e) ergänzen, weil ...

BEGRÜNDEN SIE IHRE ENTSCHEIDUNG *mit mind. 8 Stätze!*

Ich empfinde, dass diese Richtlinie RICHTIG ist, sofern Sichergestellt ist, dass die Anschlüsse von zwei unabhängigen Stromkreisläufen betrieben werden. Ebenfalls sollte es so geregelt sein, dass die System auch über das Notstromnetz funktionieren, und nicht vom "normalen" Stromnetz abhängig sind. Ebenfalls sollte die Stromversorgung so geregelt sein, dass die Notstromgeneration die Leistung auch erbringen können. Beispielsweise sollte nur die überlebenswichtigsten Gerätschaften am Notstromnetz hängen und Strom verbrauchen dürfen. Die Generatoren sollten auch in gewissen Abständen überprüft werden, ob die benötigte Strommenge(/last) auch hergestellt werden kann bzw. ob die Generatoren auch funktionieren.

Es sollten schon alle leitende Teile des Schranken untereinander Verbunden sein, jedoch sollten sie sich nicht gegenseitig beeinflussen, sodass die Funktionalität nicht mehr gegeben ist. Ein Schrank sollte auch so manipuliert werden können, dass dieser andere Schränke beeinflusst.

Aus den vorherigen Absätzen schließe ich Folgendes:

Ich würde folgende Punkte ergänzen, weil ich diese auch als relevant sehen würde:

1. Nur wesentliche (überlebenswichtige) Geräte sollten am Notstrom hängen
2. Nur überlebenswichtige Geräte sollte bei einem Stromausfall Notstrom beziehen dürfen
3. Die Notstromgeneratoren sollten die benötigte Leistung erbringen können.
4. Schränke sollten sich nicht gegenseitig beeinflussen können.
5. Manipulation eines Schranken, sollte nicht das gesamte Netz beeinflussen können.
6. Stromgeneratoren sollten in regelmäßigen Abständen überprüft werden.

Kommentar:

es wurde die Verfügbarkeit der CIA-Triade beim Stromkreis angesprochen

es wurde die Verfügbarkeit der CIA-Triade beim IP-Netzwerk NICHT angesprochen

es wurde die Vertraulichkeit der CIA-Triade NICHT angesprochen

es wurden mehrere Erweiterung angesprochen

◄ 3. schriftliche Leistungsüberpr Direkt zu: 4a. schriftliche Leistungsüberprüfung ►