Beurteilung von Richtlinien: RICHTIG oder FALSCH?

**Richtlinie für KRITIKALITÄTSANALYSE:**

*Bei der Kritikalitätsanalyse werden aus der Prozessübersicht des SPITALS diejenigen Prozesse ausgewählt, deren Ausfall oder Störung zu schwerwiegenden Verletzungen der Schutzziele der Gesundheitseinrichtung führen würden.*

***Diese Prozesse werden als kritische Prozesse bezeichnet.***

*Zur Auswahl der kritischen Prozesse sind folgende Kriterien entscheidend:*

*1. die Auswirkungen eines Prozessausfalls auf Leben und Gesundheit,*

*2. der Umfang eines Prozessausfalls,*

*3. die gesetzliche, vertragliche oder gesellschaftspolitische Relevanz der Ausfallsfolgen und dabei*

*3a. die potenziellen Auswirkungen der Verletzung der Vertraulichkeit von personenbezogenen Daten für die betroffene Person,*

*3b. die Ausfallszeit (Minuten, Stunden, Tage), an dem die Auswirkungen eines Ausfalls als kritisch anzusehen ist,*

*4. die mit einem Ausfall verbundenen wirtschaftlichen Schäden.*

*Bei der Kritikalitätsanalyse werden Bedrohungen ermittelt, die die Prozesse nach den oben angeführten Kriterien beeinflussen.*

1. *Warum ist diese Richtlinie* ***RICHTIG*** *ist oder* ***FALSCH****.*
2. *Warum ist z.B. die Bedrohung "RANSOMWARE" als kritisch, für einen Prozesse in der Gesundheitsversorgung im Spital zu bewerten.*

|  |
| --- |
| * Diese Richtlinie ist RICHTIG, weil die IKT-Systeme/Anwendungen und/oder das IKT-Netzwerk, die für kritischen Prozesse verwendet werden, durch definierte Vorgangsweise behandelt werden.   Die Vorgangsweise für die Bewertung könnte mit folgender Frage überprüft werden.  **Frage:** Sind die IKT-Systeme und das IKT-Netzwerk des Prozesses durch die Bedrohung der CIA-Triade gefährdet?   * JA, wir haben Schutzmaßnahmen gegen den Verlust der Vertraulichkeit und der Integrität getroffen. * JA, wir haben auch Redundanzen für die IKT-Systeme/Anwendungen und das IKT-Netzwerk eingesetzt. * Damit wir die Ordnungsmäßigkeit dieser Maßnahmen nachweisen können, werden dieses permanent Überwacht (Monitoring). Ist die permanente Überwachung nicht möglich, dann überprüfen wird regelmäßig abhängig von der Kritikalität des Prozesses durch Pen-Test 1 x am Tag, Woche, Monate, Halbjahr und Jahr. * Vor Einsatz oder Änderung des IKT-Systems/Anwendung und/oder des IKT-Netzwerks werden definierte Abnahme­prüfungen durchgeführt. * Beim Monitoring oder Pen-Testen ist genau definiert, WER, WIE und nach welcher ZEIT informiert wird (Meldeweg). Hierbei ist auch festgelegt, welche Eskalationen nach welcher ZEIT durchgeführt werden. * Durch die Kritikalität der Prozesse ist auch die Vorgangsweise im Katastrophenfall (K-Fall) definiert. Wir haben eine eigene Katastrophenstruktur in der IKT definiert oder können auch in die Katastrophenstruktur im Spital eingebunden werden. |

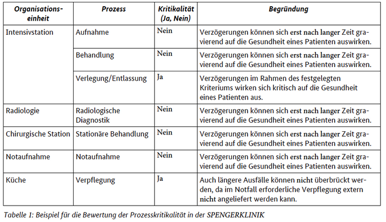
* Die Bedrohung "RANSOMWARE" ist für die Prozesse im Spital KRITISCH, weil durch die Verschlüsselung der Daten katastrophale Folgen bei der Versorgung der Patientinnen und Patienten entstehen können. Daher werden Maßnahmen getroffen, wie sie oben beschrieben sind. Ein weiterer Punkt ist das IKT-Security-Awareness-Training für das Personal und andere Personen im Spital.

## Kritikalitätsbeispiel SPITAL: RICHTIG oder FALSCH?

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.**



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

Die Richtlinie ist falsch, wenn nur eine der Beurteilung der Kritikalität aus Ihrer Sicht falsch ist.

Beurteilen Sie aus Ihrer Sicht die Kritikalität jedes Prozesses aus der Tabelle und legen Sie fest: ***richtig / falsch und warum***

b) Welche Maßnahmen leiten Sie bei der IKT-Unterstützung für diese Prozesse ab?

Die Maßnahmen müssen die CIA-Triade unterstützen.

Die Maßnahmen für die Fehler-/Störungsbehandlung müssen die Gesetze: DSGVO, MPG und NISG beachten und unterstützen

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Diese Richtlinie ist FALSCH, weil die Kritikalität bei den Prozessen der Organisationseinheit nicht immer richtig bewertet ist. Bei den unten angeführten Prozessen kann davon ausgegangen werden, dass Störungen der CIA-Triade der IKT-Systeme/Anwendungen und/oder des IKT-Netzwerks Auswirkungen mit einer Drehung um fast 180° Grad haben.     |  |  |  | | --- | --- | --- | |  | Aufnahme | Ohne Daten der Patientinnen und Patienten können „nur“ im Katastrophenfall (K-Fall) weitere Schritte im Spital durchgeführt werden, daher ist die Kritikalität **mit JA zu beantworten.** | |  | Behandlung | Ohne IKT-Systeme/Anwendungen und/oder IKT-Netzwerk können „nur“ im Katastrophenfall (K-Fall) weitere Schritte im Spital durchgeführt werden, daher ist die Kritikalität **mit JA zu beantworten.** | |  | Radio.Diagnostik | Ohne IKT-Systeme/Anwendungen und/oder IKT-Netzwerk können „nur“ im Katastrophenfall (K-Fall) weitere Schritte im Spital durchgeführt werden, daher ist die Kritikalität **mit JA zu beantworten.** | |  | Stat.Behandlung | Ohne IKT-Systeme/Anwendungen und/oder IKT-Netzwerk können „nur“ im Katastrophenfall (K-Fall) weitere Schritte im Spital durchgeführt werden, daher ist die Kritikalität **mit JA zu beantworten.** | |  | Notaufnahme | Ohne IKT-Systeme/Anwendungen und/oder IKT-Netzwerk können „nur“ im Katastrophenfall (K-Fall) weitere Schritte im Spital durchgeführt werden, daher ist die Kritikalität **mit JA zu beantworten.** | |
|  |
| |  |  | | --- | --- | | 1. Aufnahme, 2. Behandlung, 3. Radio.Diagnostik, 4. Stat.Behandlung u. 5. Notaufnahme | Ohne Daten der Patientinnen und Patienten und/oder IKT-Systeme/Anwendungen und/oder IKT-Netzwerk können „nur“ im Katastrophenfall (K-Fall) weitere Schritte im Spital durchgeführt werden, daher ist die Kritikalität **mit JA zu beantworten.** | |

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

1. Die IKT-Systeme und das IKT-Netzwerk sind durch verschiedene Bedrohungen der CIA-Triade gefährdet.
   1. Wir haben daher Schutzmaßnahmen gegen den Verlust der Vertraulichkeit und der Integrität getroffen.
   2. Wir haben daher auch Redundanzen für die IKT-Systeme/Anwendungen und das IKT-Netzwerk eingesetzt.
   3. Damit wir die Ordnungsmäßigkeit dieser Maßnahmen nachweisen können, werden dieses permanent Überwacht (Monitoring). Ist die permanente Überwachung nicht möglich, dann überprüfen wird regelmäßig abhängig von der Kritikalität des Prozesses durch Pen-Test 1 x am Tag, Woche, Monate, Halbjahr und Jahr.
   4. Vor Einsatz oder Änderung des IKT-Systems/Anwendung und/oder des IKT-Netzwerks werden definierte Abnahmeprüfungen durchgeführt.
   5. Beim Monitoring oder Pen-Testen ist genau definiert, WER, WIE und nach welcher ZEIT informiert wird (Meldeweg). **Dabei beachten wir genau die Vorgaben der DSGVO, MPG und NISG**. Hierbei ist auch festgelegt, welche Eskalationen nach welcher ZEIT durchgeführt werden.

Durch die Kritikalität der Prozesse ist auch die Vorgangsweise im Katastrophenfall (K-Fall) definiert. Wir haben eine eigene Katastrophenstruktur in der IKT definiert oder können auch in die Katastrophenstruktur im Spital eingebunden werden.

High Level Structure

