CONTECHNET
Einfach anders.

Der 20-Minuten Guide zur IT-Notfallplanung

Erste Hilfe für die IT im Krankenhaus

Inhalt

Bildnachweise:
Grafiken und weiteres Bildmaterial: CONTECHNET Ltd.

WARUM BENÖTIGE ICH ALS KRANKENHAUS EINE IT-NOTFALLPLANUNG?

DIE PROZESSE IN KRANKENHÄUSERN WERDEN IMMER KOMPLEXER UND SIND VON DER IT-INFRASTRUKTUR ABHÄNGIG.

Geschäftsprozesse und Services werden immer öfter virtualisiert und mit IT-Systemen abgebildet. Das KIS (Krankenhausinformationssystem) ist dabei das Herzstück der Krankenhäuser. Diese sollten sich also die Frage stellen, wie lange sie ohne ein funktionierendes KIS auskommen können.

Was passiert mit den Patienten, deren elektronische Patientenakte beim IT-Ausfall nicht abrufbar ist? Wie erhebe ich bei Störung meiner Systeme Labordaten und wie erhalte ich bei Ausfall meines Radiologiesystems Röntgenbilder für die anstehenden OPs?

Kommt es zu Ausfällen der IT, ist mit finanziellen Schäden zu rechnen, wenn beispielsweise ärztliche Leistungen nicht mehr abgerechnet werden können. Auch rechtliche und politische Konsequenzen sind möglich. wenn ein Krankenhaus sich beispielsweise von der Notfallversorgung abmelden muss. Damit verbunden ist auch immer die Gefährdung von Arbeitsplätzen.

Daraus resultierend ergibt sich eine immer größer werdende Verantwortung für die IT. Die IT-Abteilungen sind jedoch häufig unterbesetzt. Dadurch werden nicht selten externe IT-Dienstleister zur Unterstützung beauftragt. Auf diese Weise entstehen jedoch interne und externe Kopfmonopole, also Mitarbeiter mit exklusivem Spezialwissen. Sind diese Mitarbeiter erkrankt oder verlassen das Unternehmen, kommt es zu Know-how-Verlust.

Dem kann durch eine Notfallplanung entgegengewirkt werden, indem das Personal mit seinen Fähigkeiten aufgelistet wird. Dadurch werden Kopfmonopole sichtbar und können rechtzeitig vermieden werden. Eine IT-Notfallplanung stellt außerdem Handlungsanweisungen und Maßnahmen bereit, um in einer Notfallsituation wie z.B. einem Brand, einem Ausfall des Rechnezentrums oder einem Hacker-Angriff schnell reagieren zu können und weiterhin handlungsfähig zu sein.

ZAHLREICHE VERORDNUNGEN UND STANDARDS WIE 100-4 DES BSI, ISO 27001 ODER DIE EU-DSGVO VERLANGEN EINE NOTFALL-PLANUNG.

Die Notfallplanung ist sowohl Bestandteil der Informationssicherheit als auch des Datenschutzes und damit auch von gesetzlichen Verordnungen und Zertifizierungen. Krankenhäuser zählen aufgrund ihrer besonderen Bedeutung für das Wohlergehen der Bevölkerung zu den kritischen Infrastrukturen (KRITIS) und müssen deshalb eine Notfallplanung im Rahmen des ISMS (Informationssicherheitsmanagementsystem) einführen.

Da Krankenhäuser mit kritischen personenbezogenen Daten u.a. auf ihren Medizingeräten arbeiten, müssen diese besonders geschützt werden. Die steigende Digitalisierung und der ökonomischen Druck der Krankenhäuser, die durchgängige Betriebsfähigkeit zu gewährleisten, sind zusätzliche Anforderungen. Der große Kostendruck und die mangelnden finanziellen Ressourcen machen es Angreifern jedoch leicht, Daten abzugreifen oder ganze Prozesse lahmzulegen.

WARUM BENÖTIGE ICH ALS KRANKENHAUS EINE IT-NOTFALLPLANUNG?

EINE IT-NOTFALLPLANUNG STELLT DIE ABHÄNGIGKEITEN ZWISCHEN PROZESSEN, SERVICES UND DER IT HER.

Bei der Einführung einer IT-Notfallplanung gilt es für die Krankenhäuser zunächst die Prozesse zu identifizieren, die für den wirtschaftlichen Erfolg ausschlaggebend sind. Diese müssen im Notfall abgesichert sein. Eine funktionierende IT-Infrastruktur ist also unumgänglich. Daher müssen die entsprechenden Abhängigkeiten bekannt sein. Diese Abhängigkeiten schaffen Transparenz über die Anforderungen der Prozesse an die IT im Krankenhaus. Sicherheitslücken oder fehlende Redundanzen bei den Systemen können so aufgedeckt und behoben werden.

Die Verknüpfung der IT-Infrastruktur mit den Kernprozessen und die damit entstandene Transparenz über die Anforderungen schafft noch weitere Mehrwerte: Die Geschäftsleitung hat damit eine valide Grundlage, auf der sie Entscheidungen für zukünftige Investitionen treffen kann. Damit kann eine IT-Notfallplanung dabei helfen, Prozesse zu straffen, zu optimieren und auf diese Weise Kosten einzusparen.

Ein weiterer Effekt bei der Einführung der IT-Notfallplanung: Mögliche Ausfallszenarien lassen sich aufstellen und mit entsprechenden Wiederanlanlaufplänen verknüpfen. Diese Szenarein können mit den Mitarbeitern in Notfallübungen trainiert werden. Die Komplexität der IT kann somit reduziert und klar definierte Ressourcen und Handlungsanweisungen im Notfall bestimmt werden. Damit ist jeder Mitarbeiter informiert, für welchen Prozess wer verantwortlich ist und im Notfall kontaktiert werden muss. Dies ist im Schadensfall wesentlich für den Fortbestand des Krankenhauses, da zeitnah reagiert werden kann.

Wer sich also im Vorfeld eines Notfalls Gedanken über die möglichen Szenarien macht, Wiederanlaufpläne erstellt und das Vorgehen mit den Mitarbeiter trainiert, der ist für den Ernstfall vorbereitet. Kommt es dennoch zu einem Notfall, wissen alle Mitarbeiter, was sie zu tun haben und wie sie die Systeme wieder zum Laufen bringen. Durch das effiziente Handeln aller Beteiligten werden die finanziellen Schäden minimiert und auch rechtliche Konsequenzen vermieden.

Die wichtigsten Mehrwerte im Überblick:

- Transparenz über die Abhängigkeiten der Prozesse von der IT-Infrastruktur
- Schwachstellen bei den IT-Systemen werden erkannt und können zeitnah behoben werden
- Kopfmonopole werden rechtzeitig identifiziert
- Zielgerichtete Investitionen sind möglich
- Notfallhandbuch wird erstellt
- Minimierung der finanziellen und rechtlichen Konsequenzen

UMSETZUNGSMÖGLICHKEITEN IM VERGLEICH

Es bestehen unterschiedliche Varianten für die Umsetzung einer IT-Notfallplanung. Im Folgenden werden die drei meist verbreitetsten Methoden mit ihren Vor- und Nachteilen vorgestellt:

Traditionell in Office

Die Umsetzung einer IT-Notfallplanung soll in vielen Organisationen kein Geld kosten. Aus diesem Grund werden oft Excel und andere Office-Anwendungen genutzt, die im Krankenhaus bereits vorhanden sind. Diese führen allerdings zu einem enormen Pflegeaufwand, da die Daten an mehreren Stellen aktuell gehalten werden müssen. Die doppelte Datenpflege demotiviert wiederum die Mitarbeiter und ist sehr fehleranfällig. Außerdem sind solche Dokumente schnell nicht mehr aktuell und dadurch wertlos.

Es besteht weiterhin die Gefahr, den Überblick zu verlieren. So werden beispielsweise Personen als Verantwortliche eingetragen, die gar nicht mehr im Unternehmen tätig sind oder es wird auf Dokumente verlinkt, die bereits veraltet sind. Eine Struktur bei der Erfassung der Daten ist damit nicht vorhanden. Somit liefert diese Vorgehensweise keine sinnvollen Synergien im Tagesgeschäft.

Was also zuerst als kostengünstigste Methode erscheint, ist am Ende die zeitaufwendigste und somit auch teuerste Variante zur Umsetzung einer IT-Notfallplanung.

Externe Beratungsunternehmen

Um eine IT-Notfallplanung einzuführen, greifen viele Krankenhäuser auf externe Berater zurück. Diese bringen das benötigte Fachwissen mit und sind für die Implementierung der Notfallplanung zuständig. Allerdings wählen externe Berater oft sehr aufwändige Methoden, um möglichst viele Beratertage abrechnen zu können. Zusätzlich liegt bei diesem Vorgehen das gesamte Wissen bei nur einer Person. Sollte der Berater das Krankenhaus verlassen, müssen sich andere Mitarbeiter in die Thematik einarbeiten oder es wird ein neuer Berater beauftragt, der ebenfalls Zeit benötigt, um in das Projekt einzusteigen. Deshalb sind auch mit externen Beratungsunternehmen Risiken verbunden.

Softwarelösung

Eine weitere Möglichkeit ist die Nutzung einer Softwarelösung. Diese gibt die Vorgehensweise vor und erleichert so die Umsetzung erheblich. Die tägliche Arbeit wird reduziert, da Aktualisierungen automatisch mithilfe von Schnittstellen eingepflegt werden können. Dadurch werden die Daten nur an einer Stelle erfasst und sind jederzeit auf dem aktuellen Stand. Somit lassen sich personelle und finanzielle Ressourcen einsparen.

Auf Knopfdruck werden umfangreiche Berichte erzeugt und dienen als Nachweis für den Wirtschaftsprüfer. Der Beratungsaufwand wird durch eine Softwarelösung deutlich gesenkt. Dadurch entfällt die Abhängigkeit zu externen Beratern. Die Auflistung des Personals mit den entsprechenden Fähigkeiten macht Kopfmonopole sichtbar und sorgt dafür, dass diese rechtzeitig behoben werden können.

Darüber hinaus schafft eine softwaregestützte Lösung durch die Verknüpfung von Prozessen und der IT-Infrastruktur Transparenz im Krankenhaus. Mit dem Wissen über die Anforderungen an die IT-Infrastruktur können Investitionen zielgerichtet getätigt werden. Ein weiterer Vorteil: Dokumente und Verträge werden direkt in der Lösung verwaltet. Aufgaben können über eine Web-Anwendung an die entsprechenden Mitarbeiter delegiert werden und ermöglichen das dezentrale Arbeiten.

Eine Softwarelösung ist also bei der Anschaffung mit höheren Kosten verbunden. Jedoch wird der Pflegeaufwand deutlich minimiert und es entstehen zahlreiche Mehrwerte bei der täglichen Arbeit.

WIE ERSTELLE ICH EINE PROZESSORIENTIERTE IT-NOTFALLPLANUNG?

VORBEREITUNG

1. Sensibilität im Krankenhaus und bei den Entscheidern schaffen

Eine der wichtigsten Voraussetzungen für die Einführung einer IT-Notfallplanung ist, dass das Management hinter dem Projekt steht. Ohne die Unterstützung der Geschäftsführung und die Bereitstellung von Ressourcen und einem entsprechenden Budget wird das Projekt nicht funktionieren. Die Umsetzung der IT-Notfallplanung ist aber auch im eigenen Sinne der Geschäftsführung: Sie kann gegenüber den Geschäftspartnern, dem Wirtschaftsprüfer oder Versicherungen nachweisen, dass sie die Organisation auf den Notfall vorbereitet und sich mit den Ausfallszenarien auseinandergesetzt hat.

2. Geltungsbereich bestimmen und Vorgehensweise wählen

Zu Beginn des Projektes sollte der Geltungsbereich der Notfallplanung definiert werden. Anschließend muss ein Projektteam bestimmt und die Vorgehensweise festgelegt werden. An dieser Stelle sollte sich das Krankenhaus auch überlegen, ob es ein Beratungsunternehmen engagiert oder eine Softwarelösung anschafft.

UMSETZUNG

1. Prozessaufnahme

Kernprozesse sind die Hauptaufgabe des Krankenhauses und erwirtschaften den Umsatz. Zusätzlich verursachen diese beim Ausfall finanzielle Schäden oder starken Reputationsverlust. Aus diesem Grund sollten diese im ersten Schritt erfasst werden. Es ist ratsam, zur Definition mit der Geschäftsleitung zu sprechen und die fünf bis zehn wichtigsten Prozesse zu definieren.

Da die Kernprozesse im Krankenhaus oft noch nicht definiert sind, ist der einfachste Ansatz, die Prozesse aus der Verfahrensbeschreibung heranzuziehen. Für diese Prozesse müssen Verantwortliche und Stellvertreter bestimmt werden. Anschließend wird definiert, wie lange diese Prozesse maximal ausfallen dürfen, bis das Unternehmen einen verheerenden wirtschaftlichen Schaden erleidet. Damit ist die **Soll-Wiederanlaufzeit** festgelegt. Im Anschluss werden die Ausfallszenarien betrachtet, um auf diese Situationen entsprechend vorbereitet zu sein. Dabei empfiehlt es sich, zuerst den IT-Totalausfall darzustellen und danach die Ausfallszenarien von einzelnen Services wie die Domäne, KIS oder die Telefonanlage anzulegen. Der Vorteil bei dieser Vorgehensweise: Es wird bereits ein Gesamt-Wiederanlaufplan erstellt. Auf einen Blick ist also sichtbar, welche Komponenten notwendig sind, um das ausgefallene System wieder hochfahren zu können.

Beispiele für Ausfallszenarien sind:

intern:
- Ausfall der Aufnahme der Patienten
- Ausfall des Rechenzentrums
- Ausfall der Radiologie
- Ausfall der Laboratorien

extern:
- Stromausfall
- Feuer
- Pandemie

2. Schadensdefinition

Im nächsten Schritt geht es um die Definition des Schadens im Notfall. Zuerst sollten Krankenhäuser sich die Frage stellen: Kann die Arbeit trotz eines Ausfalls der IT fortgesetzt werden?

WIE ERSTELLE ICH EINE PROZESSORIENTIERTE IT-NOTFALLPLANUNG?

Wenn die Frage mit „Ja“ beantwortet wird, sollten organisatorische Maßnahmen vorbereitet werden.

Ein Beispiel dafür wären Checklisten und Laufzettel für Patienten, um die erbrachten Leistungen zu dokumentieren und später nachpflegen und abrechnen zu können. Zur Festlegung, wie lange ein solcher Prozess ausfallen darf, muss der Schaden definiert werden. Dieser kann errechnet werden, indem geschätzt wird, welche zeitlichen, personellen und finanziellen Ressourcen benötigt werden, um die zuvor schriftlich erfassten Daten nachträglich in ein entsprechendes System wie z.B. KIS einzupflegen. Je nach Länge des Ausfalls steigt dieser Aufwand und es gehen auch mehr Daten verloren.

Wenn die vorangestellte Frage mit „Nein“ beantwortet wird, muss der Jahresumsatz des Prozesses auf den Stundenumsatz heruntergebrochen werden. Dabei sollte beachtet werden, dass der Schadenssatz am Wochenende variieren kann, da hier oft vermindert oder gar nicht gearbeiten wird.

3. Rechtliche Auflagen

In diesem Schritt muss überlegt werden, ob rechtliche Konsequenzen auf das Krankenhaus zukommen, wenn die IT längere Zeit ausfällt. Diese können Klagen von Patienten, Ärzten, Besuchern, Firmen oder Institutionen sein, die durch die Störung geschädigt wurden. Ein Beispiel dafür ist ein Notfallkrankenhaus, das sich von der Notfallversorgung abmelden muss und deshalb nicht mehr von Krankenwagen angefahren wird. Die Information über die zusätzlichen Auflagen ist notwendig, um im Schadensfall Folgeschäden zu vermeiden. Dabei soll sich der Notfallverantwortliche keine umfangreichen Dokumente durchlesen müssen, sondern kurze und prägnante Informationen erhalten.

4. Personalerfassung

Bei der Personalerfassung müssen alle internen und externen Mitarbeiter aufgelistet werden, die zur Wiederherstellung der IT-Systeme und für die Leitung im Notfall erforderlich sind.

Dabei sind folgende Informationen wichtig:

- Name und Abteilung/Aufgabenbereich
- Tätigkeitsort und Firmenzugehörigkeit
- Kontaktdaten (auch privat): Telefon-nummer, Mobilnummer, E-Mail-Adresse
- Fähigkeiten des Mitarbeiters (aus rechtlichen Gründen nicht die Qualifikationen wie Abschlüsse oder Zertifikate, sondern nur die Befähigung zu einer Aufgabe)

5. Personalzuteilung

In vielen Krankenhäusern ist es schon vorgekommen, dass sich im Notfall niemand für einen Prozess verantwortlich gefühlt hat. In anderen Fällen war der Verantwortliche im Urlaub und es gab keine klaren Anweisungen, was im Notfall zu tun ist. Aus diesem Grund wird im fünften Schritt das zuvor erfasste Personal den Notfallteams und Krisenstäben zugeordnet.

Als Krisenstab wird eine provisorisch einberufene Leitung im Krisenfall verstanden, die die Notfallpläne und deren Ausführung koordiniert, überwacht sowie notwendige Entscheidungen trifft. Im Notfall muss der Krisenstab entsprechend der jeweiligen Gefahr zusammengestellt werden und Kontakt zu Behörden und der Presse halten.

Ein Notfallteam besteht aus den ausführenden Mitarbeitern, die die Notfallpläne umsetzen und beispielsweise die ausgefallenen IT-Systeme wieder zum Laufen bringen. Diese wissen durch die Notfallpläne, wie sie im Ernstfall vorgehen müssen.

WIE ERSTELLE ICH EINE PROZESSORIENTIERTE IT-NOTFALLPLANUNG?

Im Krisenstab sowie im Notfallteam werden jeweils ein Leiter und ein Stellvertreter bestimmt sowie die Aufgaben innerhalb des Teams definiert z.B. die Kommunikation mit der Presse.

Sollte ein Mitarbeiter das Unternehmen verlassen oder von seinen Aufgaben entlastet werden, kann ein anderer Mitarbeiter mit den gleichen Fähigkeiten seinen Aufgaben zugeordnet werden. Bei einer Softwarelösung ist hier der Vorteil, dass dieser Personaltausch mit nur einem Mausklick möglich ist.

6. Aufnahme von Dokumenten/Bildern

In einem Notfall ist es erforderlich, dass Dokumente auffindbar sind und sich nicht an unterschiedlichen Stellen im Krankenhaus befinden und erst mühsam zusammengesucht werden müssen. Aus diesem Grund ist es wichtig, bei einer Notfallplanung alle relevanten Dokumente wie z.B. Verträge und Lizenzen zu erfassen und in das Notfallsystem zu importieren. Auch Bilder sind von Vorteil, wenn es zum Beispiel um Lagepläne, Schaltpläne oder Serverschränke geht. Somit sind im Notfall alle wichtigen Dokumente und Bilder an einem zentralen Ort hinterlegt und schnell auffindbar.

Kritisch sind dagegen die Fälle, bei denen Wartungsverträge mit garantierten Wiederherstellungszeiten abgelaufen sind, weil sich niemand um die Verlängerung gekümmert hat. Deshalb sollte auch die Aktualität der Dokumente überwacht werden.

7. Aufnahme der Infrastruktur

Damit die IT-Infrastruktur im Notfall wieder hochgefahren werden kann, müssen alle für den Wiederanlauf relevanten Systeme erfasst werden. Dazu gehören IT-Systeme, Räume, Gebäude, Verbindungen, Anwendungen, Schnittstellen und organisatorische Maßnahmen. Beispiele dafür sind USVs, Server, Firewalls oder Internetdienste. Zur Vereinfachung können auch an dieser Stelle Importer und Schnittstellen wie Inventory-, NAC- oder Monitoring-Tools genutzt werden. So wird die gesamte IT-Infrastruktur inklusive der Komponenten, Software sowie Dienste automatisch importiert. Dies reduziert den Erfassungs- und Pflegeaufwand um bis zu 70%.

Die Infrastruktur sollte am besten nach ihrem physikalischen Standort erfasst werden. Damit weiß der Notfallverantwortliche, in welchem Serverraum sich der entsprechende Server befindet. Zusätzlich benötigt der Verantwortliche alle Spezifikationen und Funktionen der Systeme, um im Ernstfall Ersatzbestellungen auslösen zu können. Dafür sind u.a. folgende Daten notwendig:

- Hostname
- Systemlieferant
- Seriennummer
- Komponenten des Systems
- Softwareversion
- Login-Daten
- Datensicherung
- Wartungs- und Lizenzverträge

Die Aufgabe besteht nun darin, Wiederanlaufprozeduren für alle IT-Systeme festzulegen. Hier gilt es vor der Erstellung zu überdenken, wie bestimmte immer wiederkehrende Vorgänge standardisiert werden können. Zur Vereinfachung können bei Nutzung einer Softwarelösung Vorlagen im „Prozedurenmanagement“ erstellt werden. So wird für gleichartige Systeme ein einziger Wiederanlaufplan erstellt, der wiederrum weiteren Systemen zugeordnet werden kann.

8. Infrastrukturzuteilung

Im nächsten Schritt wird die IT-Infrastruktur den Prozessen zugeordnet. Dadurch ist es möglich, beim Ausfall eines IT-Systems sofort einen Überblick zu erhalten, welche Prozesse beeinträchtigt sind. Andersherum kann aber

genauso bestimmt werden, welche IT-Systeme überprüft werden müssen, wenn ein Service wie z.B. E-Mail ausfällt. Anschließend können die Wiederanlaufpläne für die einzelnen Prozesse angelegt werden. Dabei ist es am einfachsten, wenn mit dem IT-Totalausfall begonnen wird. Alle folgenden Prozesse sind in diesem enthalten und müssen dann nur noch als Teilausschnitt abgebildet werden. Dabei sollten auch organisatorische Maßnahmen als Teilschritte im Wiederanlaufplan integriert werden. Also beispielsweise die Einberufung des Krisenstabs oder die Kommunikation mit der Presse.

Wenn alle Wiederanlaufpläne für die unterschiedlichen Ausfallszenarien erstellt wurden, ist die **Ist-Wiederanlaufzeit** definiert. Diese muss mit der Soll-Wiederanlaufzeit aus Schritt 1 abgeglichen werden. Besteht hier eine Differenz, sollte mit dem Management über Möglichkeiten zur Angleichung gesprochen werden.

LAUFENDER BETRIEB

1. Notfallübungen

Anhand von ausgewählten Notfallszenarien sollte getestet werden, ob die erfassten Daten realistisch sind. Besonders Notfall-Übungen für Backups zeigen oft, dass bei der Wiederherstellungszeit zu optimistisch herangegangen wurde.

Übungen mit den Mitarbeitern stellen außerdem sicher, dass im Notfall jeder Verantwortliche weiß, was zu tun ist und wie er mit dem Notfallplan umzugehen hat.

2. Aufgabenmanagement

Durch das Delegieren von Aufgaben wird die Erstellung einer IT-Notfallplanung erleichtert. Deshalb sollte bei der Auswahl einer Umsetzungsmethode auch auf ein benutzerfreundliches Aufgabenmanagement geachtet werden. In diesem werden die Aufgaben erstellt, zugeteilt und überwacht. Der Auftragsteller kann somit Aufgaben systematisch an andere Mitarbeiter deligieren und sich über den aktuellen Bearbeitungsstand informieren. Der Mitarbeiter sieht nur die für ihn hinterlegten Aufgaben und kann diese über eine Weboberfläche bearbeiten. Dies vereinfacht das Projekt-Controlling und liefert einen nachvollziehbaren Stand der Umsetzung.

3. Weitere Schritte

Da eine IT-Notfallplanung dynamische Systeme beinhaltet, sollte sie nach der Einführung regelmäßig aktualisiert werden. Dafür müssen Revisions-Zeiträume festgelegt werden.

Bei Verwendung einer Softwarelösung zur Umsetzung der IT-Notfallplanung liefert die Software umfangreiche Analyse- und Reportfunktionen. Diese können zur Auswertungszwecken verwendet werden oder dienen als Nachweis für den Wirtschaftsprüfer. Automatische Wiedervorlagen stellen weiterhin die Aktualität der Daten sicher.

Als Ergebnis erhält das Krankenhaus damit ein Notfallhandbuch sowie ein Betriebshandbuch der IT zur internen Verwendung sowie als Dokumentation für den Wirtschaftsprüfer.

WAS PASSIERT, WENN DER ERNSTFALL EINTRITT?

Eine effektive Abarbeitung eines Notfalls setzt eine zuvor erfolgte. detaillierte und kontinuierlich gepflegte Dokumentation voraus. Bei Verwendung einer Softwarelösung erleichtern viele Automatismen die Pflege der Daten:

- Notfallplane können regelmaßig ausgedruckt und für den Notfall an einem festgelegten Ort hinterlegt werden.
- Die Softwarelösung regelmaßig auf die neueste Version updaten und für den Notfall bereitstellen (z.B auf einem Notfall-Laptop).
- Sicherstellen. dass es genügend Personal gibt, das die Softwarelösung bedienen kann.
- Ggf. einen Drucker bereitstellen. der auch im Notfall drucken kann.

Die Notfallsituation

Tritt eine Störung des betrieblichen Prozessablaufs auf. erfolgt eine Meldung an den Notfallverantwortlichen. Dieser oder ein mit der Aufgabe betrauter Mitarbeiter nimmt die Softwarelösung zur Hilfe:

1. Art des Notfalls bestimmen: Welcher Prozess ist betroffen? Welche Systeme sind betroffen?
2. Kontaktaufnahme zu dem zuvor festgelegten Krisenstab bzw. den Notfallteams.
3. Feststellung der ausgefallenen IT-Infrastruktur und beeinträchtigten Prozessen

Der Ausfallmanager

Ist ein Prozess ausgefallen, werden alle Informationen bereitgestellt, die im Notfall benötigt werden.

- Maximale Ausfallzeit und die entsprechenden Schadensdefinitionen: Wieviel Zeit bleibt, bis die maximale Ausfallzeit erreicht ist? Mit welchem Schaden ist zu rechnen?
- Darstellung aller Systeme, die in diesen Prozess mit eingebunden sind
- Die Verantwortlichen für die jeweiligen Infrastrukturobjekte sowie die Prozessverantwortlichen sind mit ihren Kontaktdaten hinterlegt

Sind bestimmte Systeme in der Infrastruktur ausgefallen. werden diese mit den beeinträchtigten Prozessen und entsprechenden Verantwortlichen sowie den notwendigen Dokumenten angezeigt:

E-Mail funktioniert noch:

> Es kann eine Notfallliste aus den jeweiligen Verantwortlichen generiert und eine E-Mail an diese versendet werden. Die Texte werden als Template hinterlegt.

E-Mail funktioniert nicht:

> Es kann ein Alarmierungsbericht mit dem Personal generiert und ausgedruckt werden. Dieser enthält eine Checkliste darüber. wer zu welchem Zeitpunkt informiert wurde.
>
> Es kann ein Bericht über den Wiederanlauf generiert werden. der ebenfalls eine Checkliste zur Wiederherstellung der Systeme enthält.

Der Wiederanlauf

Um schnellstmöglich wieder in den Normalzustand zurückkehren zu können, hilft der Wiederanlaufplan, insbesondere in der grafischen Form. Dort wird dargestellt, in welcher Reihenfolge ein Prozess oder ein Service wieder gestartet wird, wie die Abhängigkeiten der Systeme untereinander sind und mit welcher Gesamtzeit zu rechnen ist.

CHECKLISTE: 8 SCHRITTE ZUR OPTIMALEN NOTFALLPLANUNG

Risikoerfassung

- [ ] 1 Aufnahme der Kernprozesse (KP), Services und Ausfallszenarien
  - [ ] 2 Finanzieller Schaden beim Ausfall pro KP
  - [ ] 3 Rechtliche Auflagen pro KP

Notfallplanung

- [ ] 4 Aufnahme des Personals (intern und extern)
  - [ ] 5 Zuordnung Krisenstäbe zum KP
    Zuordnung Notfallteams zum KP
- [ ] 6 Aufnahme der Infrastruktur
  - [ ] 7 Erstellung Wiederanlaufpläne für Kernprozesse und Services
  - [ ] 8 Erstellung Wiederanlaufpläne für ausgewählte Schadensszenarien

☑ ... fertig!

GEMEINSAME DATENNUTZUNG FÜR IT-NOTFALLPLANUNG, DATENSCHUTZ UND INFORMATIONSSICHERHEIT

In der Informationssicherheit geht es um die Absicherung von Informationen in einer Organisation. Dafür müssen mögliche Szenarien betrachtet werden, die Einfluss auf die Sicherheit dieser Informationen haben können. An diesem Punkt greift die IT-Notfallplanung: Denn auch beim Ausfall der IT-Infrastruktur müssen Informationen gesichert werden. Der Datenschutz zielt auf die Absicherung personenbezogener Daten ab. Diese können sich wiederum auf IT-Systemen befinden. Diese Zusammenhänge zeigen deutlich, wie IT-Notfallplanung, Datenschutz und ISMS ineinander greifen.

DIE UMSETZUNG EINES ISMS FORDERT DIE ERSTELLUNG EINER IT-NOTFALLPLANUNG UND EINES DATENSCHUTZKONZEPTES.

Krankenhäuser, die sich nach der ISO 27001 zertifizieren lassen möchten, müssen sich auch mit der IT-Notfallplanung und dem Datenschutz auseinander setzen. Ist jedoch bereits eine IT-Notfallplanung im Krankenhaus implementiert, bestehen viele Vorteile, da wesentliche Bestandteile des Managementsystems bereits vorhanden sind.

So können z.B. die angelegten Prozesse, die Personaldaten mit den jeweiligen Fähigkeiten und die IT-Infrastruktur im ISMS verwendet werden. Weiterhin können bereits umgesetzte Maßnahmen aus dem Datenschutz die Einführung eines ISMS deutlich beschleunigen. Die ISO 27001 Norm fordert nämlich nicht, dass Organisationen eigene Regeln für das ISMS schaffen. Daher empfiehlt es sich am Anfang des Projektes zu schauen, welche Maßnahmen im Krankenhaus bereits vorhanden sind, die die Anforderungen der Norm schon heute erfüllen und welche noch fehlen. Auf diese Weise lässt sich die Herausforderung der Implementierung aller drei Bereiche einfach und ohne großen Aufwand bewältigen.

DIE GEWÄHRLEISTUNG VON VERFÜGBARKEIT PERSONENBEZOGENER DATEN FORDERT EINE IT-NOTFALLPLANUNG.

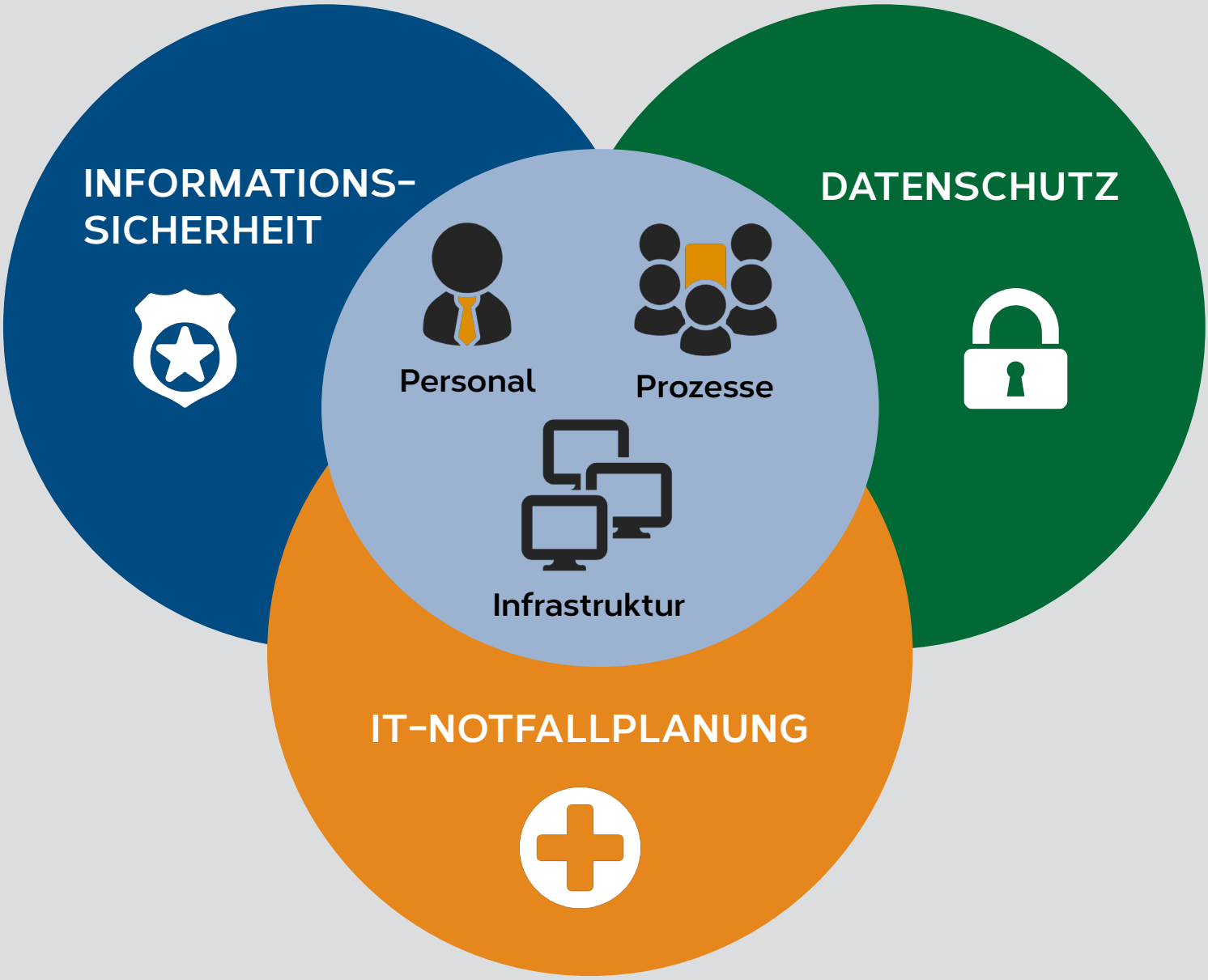
Die Implementierung einer IT-Notfallplanung setzt voraus, dass sich das Krankenhaus mit seinen Prozessen beschäftigt, die Kernprozesse definiert sowie verantwortliches Personal spezifiziert hat.

Die definierten Prozesse in der IT-Notfallplanung können als Verarbeitungen für den Datenschutz übernommen werden. Dabei lassen sich die einzelnen Prozesse auswählen und dem jeweiligen Bereich zuordnen. Diese Vorgehensweise ist in beide Richtungen möglich. Auch Personaldaten können sowohl in der IT-Notfallplanung als auch im Datenschutz verwendet werden. So kann bereits angelegtes Personal als Verantwortliche den Verarbeitungen zugeordnet werden. Die IT-Infrastruktur, also die verwendete Software für die jeweilige Verarbeitung, kann ebenfalls aus der IT-Notfallplanung importiert werden.

INTEGRIERTES MANAGEMENTSYSTEM SCHAFFT SYNERGIEN.

Mit einem integrierten Managementsystem werden die Daten zentral an einer Stelle gepflegt. Einmal angelegte Daten sind damit für alle Bereiche nutzbar. Organisationen können diese dann in der Notfallplanung, im Datenschutz sowie für ein ISMS verwenden. Mit einer Softwarelösung werden die Daten weiterhin automatisch aktualisiert. Dies verringert die Fehleranfälligkeit und den Einsatz von personellen sowie finanziellen Ressourcen. Darüber hinaus wird der riesige Dokumentationsaufwand minimiert. Auf diese Weise entstehen erhebliche Synergien.

GEMEINSAME DATENNUTZUNG FÜR IT-NOTFALLPLANUNG, DATENSCHUTZ UND INFORMATIONSSICHERHEIT



- Hohe Transparenz über den Status aller Aktivitäten
- Einheitliche unternehmensweite Datenbasis
- Vermeidung von Redundanzen
- Effizienzsteigerung
- Ressourcen-, Zeit- und Kostenersparnisse

ZUSAMMENFASSUNG

BETRACHTEN SIE IT-NOTFALLPLANUNG NICHT ALS NOTWENDIGES ÜBEL, SONDERN ALS CHANCE.

Die Einführung einer IT-Notfallplanung sollte vom Krankenhaus als Chance betrachtet werden. Durch die Zusammenhänge zwischen den Prozessen und der IT-Infrastruktur werden die Abhängigkeiten sichtbar. Wiederanlaufpläne ermöglichen eine zeitnahe Wiederherstellung der IT-Systeme und damit die Vermeidung von hohen finanziellen Schäden. Das Notfallhandbuch liefert den Mitarbeitern einen Leitfaden, um gezielt reagieren zu können und weiterhin handlungsfähig zu sein. Auf diese Weise kann das Krankenhaus vor größeren Folgen bewahrt werden.

Zudem schafft eine IT-Notfallplanung Mehrwerte bei den Mitarbeitern für ihre tägliche Arbeit und damit auch eine Motivation im Tagesgeschäft. Schwachstellen können aufgedeckt werden, die ohne die Verknüpfung der Daten nicht sichtbar geworden wären.

Durch die Nutzung einer Softwarelösung wird die Datenpflege auf ein Minimum reduziert. Das Management erkennt die Anforderungen der Prozesse an die IT-Infrastruktur und kann dadurch zielgerichteter Investitionen tätigen.

Außerdem lassen sich mit einer Softwarelösung die gesetzlichen Vorschriften einfach und ohne großen Beratungsaufwand dokumentieren und einhalten. Krankenhäusern ist es so möglich, die Umsetzung selbst in die Hand zu nehmen.

Bereits erfasste Daten können gleichzeitig für die Dokumentation der EU-DSGVO und zur Einführung eines ISMS genutzt werden. Dies schafft Synergieeffekte und macht die Einsparung von personellen und finanziellen Ressourcen möglich.

Über CONTECHNET

Die CONTECHNET Ltd., mit Hauptsitz in der Region Hannover, entwickelt und vermarktet seit zehn Jahren eigene Softwareprodukte. Als Experte auf dem Gebiet der IT-Notfallplanung ist die CONTECHNET-Suite kontinuierlich um die Lösungen in den Bereichen ISMS (Informationssicherheits-Managementsystem) und Datenschutz gewachsen – das alles „made in Germany".

Alle Softwarelösungen von CONTECHNET basieren auf einer strukturierten und vor allem praxistauglichen Vorgehensweise. Die Produkte geben die Vorgehensweise selbst vor, sie sind intuitiv zu bedienen und führen den Anwender schnell zum Ergebnis. Das Ziel ist es, komplexe IT- und Non-IT-Strukturen möglichst einfach abzubilden und das tägliche Arbeiten der Anwender mit strukturierten Managementsystemen zu erleichtern. Die entstandene Transparenz im Projektverlauf ermöglicht realistische Planungen über die Dauer und die Kosten von Einführung der Software bis zu ihrer späteren Nutzung im täglichen Geschäft.