nexus|ag

NEXUS / ISMS

Informationssicherheitsmanagementsystem

IT-Sicherheit geht alle an!

Cyberattacken, Systemausfälle, Datenlecks – was schon im privaten Bereich äußerst folgenreich sein kann, bedroht in Einrichtungen des Gesundheitswesens schlimmstenfalls Menschenleben. Deswegen muss IT-Sicherheit immer mitgedacht werden, wenn es um Digitalisierung in der Gesundheitsbranche geht!

Auch Gesetzgeber und Regierung forcieren die Thematik:

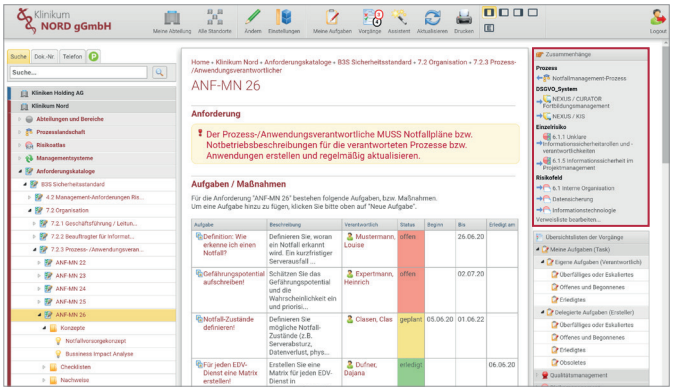
Der **§75c SGB V** verpflichtet Krankenhäuser nach dem „Stand der Technik“ angemessene Maßnahmen im Bereich der IT-Sicherheit zu ergreifen. Mit dem **Patientendaten-Schutzgesetz** greifen die scharfen Anforderungen erstmals auch die IT-Sicherheit des BSI außerhalb kritischer Infrastrukturen (KRITIS).

Ganzheitliches Informationssicherheitsmanagement mit NEXUS / ISMS: Systematisch, strukturiert, integriert

Aber wer jetzt nur an Firewalls, demilitarisierte Zonen und redundante Datenhaltung denkt: Für eine nachhaltige IT-Sicherheitspolitik sind neben den notwendigen technischen Voraussetzungen auch Maßnahmen geboten, die dazu beitragen, IT-Sicherheit organisatorisch zu verankern.

Der B3S für die Gesundheitsversorgung im Krankenhaus umfasst mehr als 160 Anforderungen – diese systematisch zu bearbeiten und nachzuhalten, kann für Gesundheitseinrichtungen eine nicht zu unterschätzende Herausforderung darstellen.

Die gute Nachricht: NEXUS / ISMS erfasst den Anforderungskatalog des B3S systematisch und pragmatisch. Es ermöglicht die Etablierung eines schlanken und übersichtlichen Managementsystems, das vorhandene Strukturen nutzt und IT-Sicherheit mit den Prozessen und Risikokatalogen Ihrer Einrichtung verknüpft.



Verknüpfung des B3S mit Prozesslandschaft und Risikokatalog

Einbinden von Normen und Anforderungskatalog

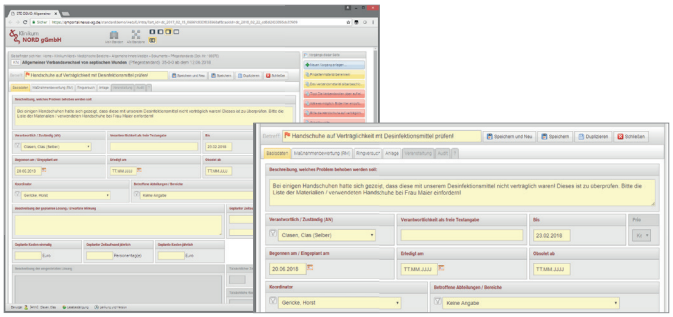
Das NEXUS / ISMS erlaubt es Einrichtungen im Gesundheitswesen, individuell und entlang den jeweiligen Bedürfnissen des eigenen Hauses, Normen und Anforderungskataloge einzubinden. Auf diesem Weg können auch individuelle Betrachtungen erfolgen - gegebenenfalls über die Basisanforderungen des B3S hinaus.

Die Verknüpfung mit einem gezielten IT-Risikomanagement ermöglicht es dem Nutzer, die Anforderungen der Normen (z.B. DIN ISO 27001) zunächst in Einzelrisiken zu übersetzen, um diese dann in einem zweiten Schritt mit entsprechenden Maßnahmen und Verantwortlichkeiten zu versehen. In der Detailansicht einer Anforderung können zusätzlich Kommentare des Teams gesammelt, Aufgaben definiert, mit Zuständigkeiten versehen und Dokumente hinterlegt werden.

Definition von Risiken und Maßnahmen

Ein integriertes Informationssicherheitsmanagement bedeutet auch: keine Duplizitätsfälle zu bereits bestehenden Managementtools. Daher werden auch bei der Verwendung von NEXUS / ISMS vorhandene Daten und Dokumente genutzt und in den Workflow des ISMS integriert.

Mit dem zentralen Maßnahmenmanagement von NEXUS / ISMS wird die Arbeit innerhalb der Organisation nicht nur vereinheitlicht und erleichtert, sondern auch klar strukturiert und kann nachgehalten werden. Gleichzeitig ermöglicht die Abbildung der Organisationsstrukturen dem User ein schnelles Finden der relevanten Normabschnitte.



Detaillierte Maßnahmenplanung in NEXUS / ISMS

Umfassend, effizient und strukturiert

Durch seinen ganzheitlichen Ansatz ermöglicht NEXUS / ISMS eine umfassende, effiziente und strukturierte Bearbeitung aller Anforderungen, Risiken und Maßnahmen unter Einbindung vorhandener Strukturen, Prozesse und Dokumente.

Das zeigt sich auch im Dashboard von NEXUS / ISMS: Durch die übersichtliche Darstellung lässt sich der Zusammenhang zwischen einzelnen Faktoren sowie deren Bewirtschaftungsgrad jederzeit überprüfen. NEXUS / ISMS ist ein Informationssicherheitsmanagementsystem mit:

+ zentraler Datenbank
+ Erinnerungs- und Aufgabenfunktionen
+ integriertem Risikomanagement
+ Übersichtslisten, Statusreports und Auswertungen
+ Anbindung eines vollwertigen Auditmanagements

Transparenz und Mitarbeitermotivation

Sichere Klinik-IT braucht sensibilisierte Beschäftigte: Für eine nachhaltige IT-Sicherheitspolitik sind neben den notwendigen technischen Voraussetzungen auch Präventionsmaßnahmen geboten, die dazu beitragen, IT-Sicherheit organisatorisch zu verankern. Im organisatorischen Bereich sind für die Prävention unter anderem das Schaffen von Awareness beim Personal oder auch die Dokumentation der IT-Landschaft des Krankenhauses wichtig. Über die automatische Veröffentlichung von Informationssicherheitsleitlinien im Intranet, durch Kommentarfunktionalitäten, Lesebestätigungen, Newsmeldungen oder ein anonymes Meldeportal werden Mitarbeiter für die IT-Sicherheit sensibilisiert und werden somit zum Teil der Lösung.

Weitere Managementtools runden die Funktionalitäten des ISMS ab. Das vollständig integrierte NEXUS / DSGVO ermöglicht beispielweise die Erfassung und Strukturierung aller Informationen, die im Zusammenhang mit der Erhebung und Verarbeitung personenbezogener Daten anfallen. Und auch die vollständige Planung von IT-Audits und Begehungen ist mit NEXUS / AUDITMANAGEMENT möglich.

Ihre Vorteile auf einen Blick

+ Übersicht der Realisierungsgrade
+ Schnelle Erfassung und Verteilung von Aufgaben
+ Vollständige Abbildung des Risikomanagementprozesses
+ Zentrale Maßnahmenverwaltung
+ Keine Einschränkung von Nutzerlizenzen
+ Vollständig webbasiert
+ Erweiterbar um weitere Managementwerkzeuge

NEXUS AG | Vertriebsniederlassung Frankfurt | Hanauer Landstr. 293 | D-60314 Frankfurt am Main
Tel. +49 (0)69 583004-200 | www.nexus-ag.de | vertrieb@nexus-ag.de

V 01 - 02.2022