

Inhalt

- 2 **Editorial**
- 4 Prävention und Transparenz
**Mit wenigen Maßnahmen
Angriffsflächen verringern**
- 6 Kurzinterview mit
Christian Schreiner, SWS
Top-down: Das Wichtigste zuerst
- 8 Daten im Gesundheitswesen sind für
Cyberkriminelle besonders attraktiv
Entscheidend ist der Mensch
- 10 E-Mail-Daten DSGVO-konform
aufbewahren
Backup oder Archivierung?
- 12 Hilfe für den Datenschutz
Sicherer Dateiaustausch tut nicht weh
- 14 Sicheres Arbeiten im Web
**Den Webbrowser vor
Cyberangriffen schützen**
- 16 Branche unter den Top-Angriffszielen
Gesundheitswesen im Fadenkreuz
- Anbieter**
- 18 Risikopatient IT
**Eine gute Vorsorge sorgt für
Cybersicherheit im Krankenhaus**
- 20 **MailStore Server und die
datenschutzkonforme E-Mail-
Archivierung im Gesundheitswesen**
- 22 **IT-Sicherheit im Krankenhaus -
so geht's**
- 24 **B3S Gesundheit für Krankenhäuser mit
QSEC am Beispiel Harzkllinikum
Dorothea Christiane Erxleben GmbH**
- 26 Sicherer Umgang mit Daten
**DSGVO-konforme Digital-Workplace-
Lösung - Ihr Rezept für einen
sorgenfreien Klinikalltag**
- 28 Digitale Sensibilisierung
**Der Faktor Mensch in der
Cybersicherheit:
Mitarbeitersensibilisierung im
Gesundheitssektor**
- 30 Vertraue niemandem!
**Zero Trust: Unverzichtbar für alle
Accessverfahren**
- 32 PC-Prophylaxe:
**Wie Krankenhäuser ihre Netzwerke
sichern können**
- 34 Aufbau einer gehärteten IT-Security-
Infrastruktur
**Case Study: indevis unterstützt Klinikum
Lippe nach Cyberangriff**
- 36 **Medizingeräte - die unterschätzte
Gefahr**
Wenn Cyber-Security auf
Patientensicherheit trifft
- 38 **Die drei Säulen für sicheren Fernsupport
im Gesundheitswesen**
- 40 **Man kann sich nur gegen das
verteidigen, was man sieht**
Die IT-Sicherheit in Krankenhäusern
benötigt den Blick auf Netzwerk und
Endpunkte.
- 42 Business Continuity
**Informationssicherheit:
Aufrechterhaltung des Betriebs ist von
zentraler Bedeutung**