

# CYBERANGRIFFE – DIE SCHONZEIT IST VORBEI !

Krankenhäuser leiden verstärkt unter Ransomware-Angriffen.



Bundesverband der  
Krankenhaus-IT-Leiterinnen/Leiter e.V.

Kontakt:  
Jürgen Flemming  
Pressereferent  
E-Mail: [Flemming@kh-it.de](mailto:Flemming@kh-it.de)  
[www.kh-it.de](http://www.kh-it.de)

In den vergangenen Wochen haben die erfolgreichen Angriffe auf die IT-Infrastruktur von Krankenhäusern massiv zugenommen. Alle Angriffe erfolgten unter Ausnutzung bekannter Sicherheitslücken, oft in Verbindung mit Phishing-Mails. Die Opfer werden dann mit zwei Bedrohungen erpresst: einerseits die Verschlüsselung wichtiger Daten, andererseits aber die Veröffentlichung der Patientendaten.

Gerade in Krankenhäusern werden sehr viele und oftmals sehr spezialisierte Anwendungen betrieben. Keine Krankenhaus-IT ist in der Lage, alle diese Anwendungen souverän mit eigenem Personal im 1st- und 2nd-Level-Support zu betreiben. Für viele Anwendungen ist die IT nur Anlaufstelle für Fehlermeldungen, die dann an den jeweiligen Hersteller oder Support-Dienstleister weitergegeben werden.

Die Einführung und Nutzung eines ISMS (Informations-Sicherheits-

management-System) gehört zusammen mit der Installation eines Informations-Sicherheitsbeauftragten zu den wichtigsten Maßnahmen. Darüber hinaus sollten die „9 goldenen Grundregeln der Häuslebauer“ berücksichtigt werden.

Seit Jahren ist eigentlich klar: Es ist nicht die Frage, ob ein Haus gehackt wird, sondern nur, wann.

Eingedenk dieser Aussage muss jedes Krankenhaus sich ernsthaft mit seiner Resilienz auseinandersetzen. Welche Prozesse greifen bei einem Ausfall des KIS? Wie wird der Ausfall des PACS gehandhabt? Welche Prozesse ermöglichen den Basisbetrieb der Notaufnahme und des restlichen Krankenhauses auch im Falle einer erfolgreichen Cyberattacke?

Viele dieser Fragen sind für die Patient:innen und das Krankenhaus von existenzieller Bedeutung. KRITIS-Häuser müssen sich inzwischen qua Definition mit diesen Fragen und dem damit verbundenen Business Continuity Management auseinandersetzen. Allen anderen Häusern, aber auch Unternehmen und öffentlichen Einrichtungen ist dringend anzuraten, genau diese Fragen zu diskutieren und die Lösungen dazu immer wieder zu proben. So wie im Krankenhaus die monatliche Stromprobe gesetzlich gefordert ist, sollte jedes Krankenhaus mindestens einmal pro Jahr den Notbetrieb ohne IT üben.

## KH-IT-VERBANDSTERMINE 2024

### Frühjahrstagung 2024

15.–16.05.2024:

Frühjahrstagung in Ihringen bei Freiburg

### Herbsttagung 2024

19.–20.09.2024:

Herbsttagung in Andernach

### Seminare

Die Seminare sind aktuell in Planung, u.a.: Rechtsseminare, NIS2 und Führungskräfteausbildung

Alle Termine und Inhalte auf der Webseite des KH-IT und in der XING-Gruppe.

## ÜBER DEN KH-IT

Der Bundesverband der Krankenhaus-IT-Leiterinnen/Leiter e.V. ist der Berufsverband der Krankenhaus-IT-Führungskräfte. Mit unseren etablierten Veranstaltungen bieten wir den Mitgliedern eine werthaltige Plattform für den Austausch untereinander, die Auseinandersetzung mit aktuellen Themen und Perspektiven für die Entwicklung und Zukunft der Informationstechnik im Krankenhaus. Bei Interesse finden Sie weitere Informationen auf unserer Webseite.

[www.kh-it.de](http://www.kh-it.de)

### Die 9 goldenen Sicherheits-Regeln der Häuslebauer:

1. Sicherheitstechnik nach „Stand der Technik“ einbauen
2. Ins Haus darf nur, wer dir bekannt ist
3. Gib nur Leuten den Schlüssel, denen Du vertraust!
4. Lass die Leute nur dahin, wo Sie mit Deinem Einverständnis etwas machen dürfen!
5. Schließ ein, was andere nichts angeht!
6. Dokumentiere Deine Wertsachen
7. Lass niemanden ohne dein Einverständnis etwas mitnehmen!
8. Bau eine Alarmanlage ein, wenn Du nicht alles kontrollieren kannst!
9. Regele schriftlich, was zu regeln ist!