

CYBER DEFENSE

SYSTEMATISCH, SCHNELL, ERSCHWINGLICH

1. VORBEUGEN

- Orientierungsworkshop IT-Sicherheit: Vorortinterview ca. 1,5 Tage, Analyse des IST-Zustands, priorisierte Handlungsempfehlungen
- Penetrations-Test: Prüft Web-Applikationen, Netzwerk oder simuliert eine Cyber-Attacke, Handlungsempfehlung

2. ERKENNEN

- Ergänzen von etablierten Sicherheitstechnologien wie z. B. Endpoint Security, Firewalls um das Korrelieren von Incidents und Events
 - Siehe hierzu unser Angebot Advanced Cyber Defense unter Nr. 4



4. VORHERSAGEN

- Advanced Cyber Defense: Managed Service aus der Telekom-Cloud (alternativ auch on premise)
- Netzwerk-Sicherheits-Monitoring + vorhandene Logs (z. B. Firewall, MS Active Directory) werden korreliert (Security Incident and Event Management), Reporting + monatl. Reviews

3. REAGIEREN

- Incident Response Service: Bei Angriffen stehen über eine Notfallrufnummer versierte Ansprechpartner der Telekom zur Verstärkung der Krankenhaus-IT bereit.
- z. B. 4 Stunden telefonische Reaktionszeit und inklusive 64 Consulting-Stunden für Reaktion auf einen Intrusion Incident, forensische Analysen und Malware Analysen

EXPERTENKONTAKT

E-Mail: info@telekom-healthcare.com

HERAUSGEBER

Deutsche Telekom AG
Telekom Healthcare Solutions
53262 Bonn



HEALTHCARE SOLUTIONS