

**STARTERPAKET**

**IS4IT**  
KRITIS

**KENNEN SIE  
DAS SCHWÄCHSTE GLIED  
IN IHREM NETZWERK?**

**SCHWACHSTELLENSCAN DES INTERNEN NETZWERKES  
ZUM PROAKTIVEN SCHUTZ IHRER IT**

# STARTERPAKET „WIE SICHER SIND IHRE IT-SYSTEME?“

## SCHÜTZEN SIE PATIENTENDATEN UND ARBEITSABLÄUFE IHRER KLINIK

### IHRE AUSGANGSLAGE

- Die Vermeidung erfolgreicher Hackerangriffe hat für Sie höchste Priorität.
- Arbeitsprozesse im Krankenhaus dürfen keinesfalls durch den Ausfall von IT-Systemen gefährdet werden.
- Sie müssen Patientendaten optimal schützen.
- Die aktuelle Nachrichtenlage im Bereich Cyber-attacken beunruhigt Sie.
- Sie müssen mit knappem Budget IT-Sicherheit so wirtschaftlich wie möglich umsetzen.
- Sie haben kein internes Security-Team und Ihr Budget verhindert den Einsatz teurer Berater.
- Ihren IT-Mitarbeitern fehlt die Zeit, sich mit aktuellen Bedrohungslagen auseinanderzusetzen.
- Sie müssen sicherstellen, dass alle gesetzlichen Regularien eingehalten werden.

### UNSER ANGEBOT

- Der erste Schritt: Schwachstellenscan Ihrer internen Netzwerke

### STARTERPAKET

**ab 2.990 € zzgl. MwSt.**

Sie möchten mehr erfahren, wie Sie sich optimal schützen können?  
Kontaktieren Sie uns unter [sec@is4it.de](mailto:sec@is4it.de)

**IS4IT** KRITIS  
IS4IT KRITIS GmbH  
telefon +49 6261 31944-0  
[info@is4it-kritis.de](mailto:info@is4it-kritis.de)

**IS4IT**  
IS4IT GmbH  
telefon +49 89 6389848-0  
[sec@is4it.de](mailto:sec@is4it.de)

**IS4IT** SCHWEIZ  
IS4IT Schweiz AG  
telefon +41 41 7200090  
[info@is4it.ch](mailto:info@is4it.ch)

### LEISTUNGSUMFANG

- Kick-off-Workshop zur Abstimmung des Scopes
- Schwachstellenscanning aller internen Systeme im jeweils angeschlossenen Netzsegment (Patchstände, schwache Passwörter und einfache Konfigurationsfehler)
- Dokumentation der ermittelten Schwachstellen
- Übersicht der Handlungsempfehlungen

### IHR NUTZEN

- Überblick über Ihre IT-Systeme im Netzwerk und deren Schwachstellen
- Objektive Umsetzung dank externer Expertise
- Schaffung eines technischen IT-Sicherheits-Grundniveaus
- Höhere Datensicherheit und reduzierte Risiken



**HanseSecure**  
Exploit Hunter

Was erwartet Sie?

### Telefonischer Kick-off zur Festlegung

Zeitplan

Scope

Benennung kritischer Systeme

Organisatorisches (Internetzugriff, NAC etc.)

Bei Bedarf Abstimmung mit externen Partnern

### Organisatorische Vorbereitung

Aufbereitung und Überprüfung der gemeldeten IP-Adressen und Domainnamen

Aktualisierung der Infrastruktur für den Schwachstellenscan

Auftragsbezogene Lizenzierung der Software

### Testphase

Scanning der Systeme

Vulnerability Assessment der Systeme

### Abschluss

Auswertung der Scanergebnisse und Dokumentation

Übermittlung des Abschlussberichts

Zertifikate/Siegel der IS4IT Kritis GmbH

**TeleTrust**  
Pioneers in IT security.  
Bundesverband IT-Sicherheit e.V.

**SecurITy**  
made in Germany

Allianz für  
Cyber-Sicherheit