Informationstag "Umsetzung des IT-Sicherheitsgesetzes in der Unternehmenspraxis"

Gemeinsame Veranstaltung von TeleTrusT, bevh und BISG

Berlin, 29.11.2016

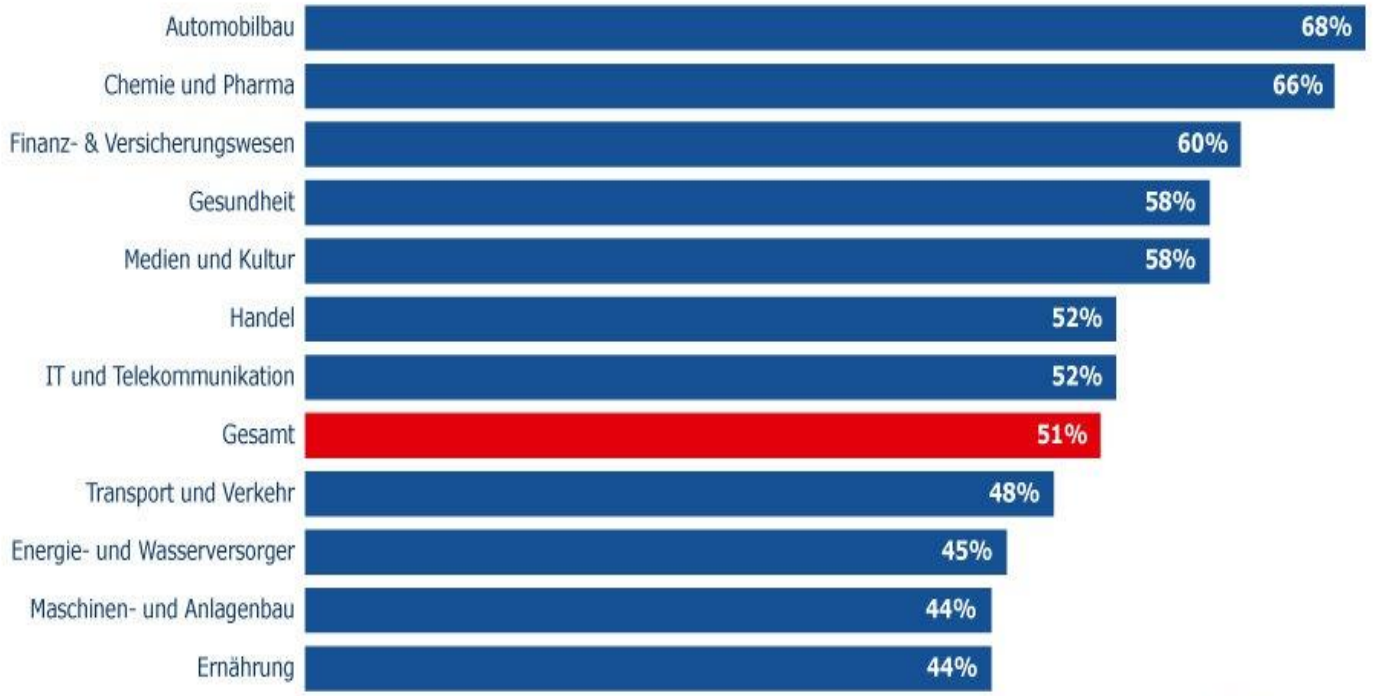
Sichere Kommunikation im Gesundheitswesen

Nikolaus Schrenk | KBO | Leitung Governance Consulting

Andreas Liefeith | procilon GROUP

Angriffe auf jedes 2. Unternehmen

Innerhalb der letzten 2 Jahre von Datendiebstahl, Wirtschaftsspionage oder Sabotage betroffene Branchen (ohne sonst. Industrie- und Dienstleistungsbranchen)



Quelle: Bitkom Research, 2015

Problemstellung, Vision & Mission

Vom ungesicherten Datenaustausch zur sicheren Klinikkommunikation

Überblick

- **über kbo**
- Ausgangslage
- Zieldefinition
- Umsetzung
- Fazit

Über kbo

- Verbund von Kliniken und ambulanten Einrichtungen für Psychiatrie, Psychotherapie und Psychosomatik für Kinder, Jugendliche und Erwachsene, Neurologie und Sozialpädiatrie
- 5.900 Mitarbeiter - rund 3.000 Betten/Plätze – etwa 80.000 Patienten jährlich
- stationäre, teilstationäre und ambulante Leistungen – wohnortnah in ganz Oberbayern an über 25 Standorten

Überblick

- über kbo
- **Ausgangslage**
- Zieldefinition
- Umsetzung
- Fazit

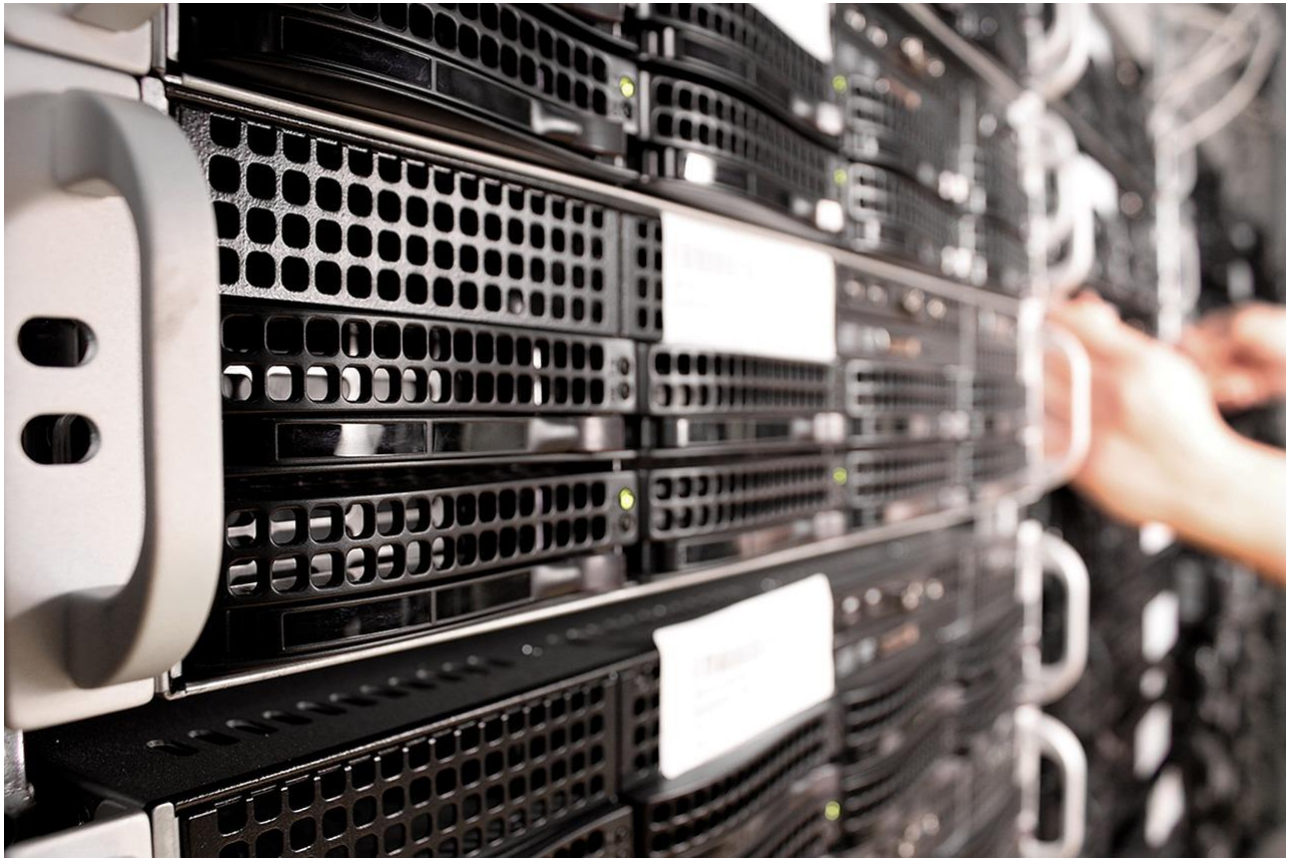
Ausgangslage

Rechtliche Aspekte

- Persönliche und sachliche Verhältnisse zu einer Person sind **schützenswert**
- Gesundheitsdaten sind im Sinne des Bundesdatenschutzgesetzes und des bayerischen Krankenhausgesetzes **besonders schützenswert**
- Die Offenbarung von Gesundheitsdaten, die im Rahmen Patienten / Arzt – Verhältnis (Schweigepflicht) erhoben wurden, ist nach § 203 StGB **strafbar**
- "Unternehmsinterna" unterliegen bei öffentlich-rechtlichen Unternehmen der Verschwiegenheit, Aussagebefugt ist nur die oberste Leitung und beauftragte Personen

Ausgangslage (2)

Krankenhäuser sind im Sinne von IT hochkomplexe Unternehmen



Ausgangslage (2)

Krankenhäuser sind im Sinne von IT hochkomplexe Unternehmen

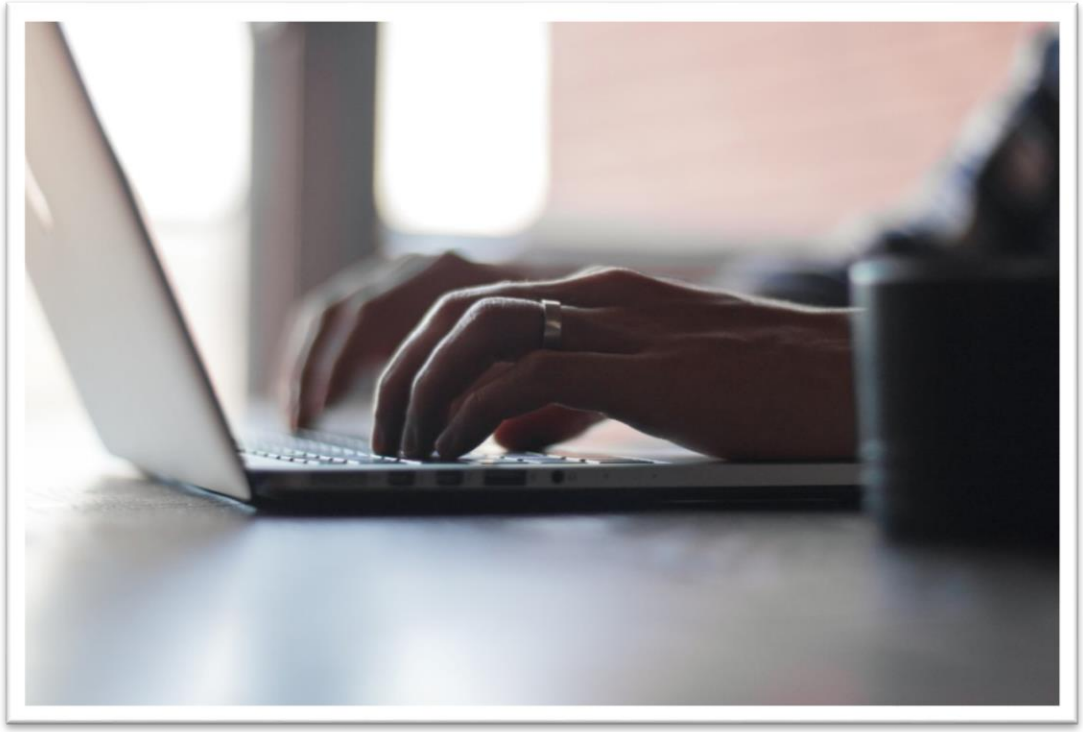
- hohe Vernetzung in der Klinik
- großer Informationsfluss zwischen Arzt / Pflege / Therapieeinheiten über Stationen / Gebäude und Organisationseinheiten hinweg
- Hohe logistische Herausforderungen
  - Patienten & Leistungserbringer und Informationen zum richtigen Zeitpunkt am richtigen Ort
  - unterstützende Leistungen und Informationen zum Patienten zum richtigen Zeitpunkt und am richtigen Ort
  - + bekannte Kommunikation im Sinne der betriebswirtschaftlichen Unternehmensführung

= heterogene IT Landschaft, die hauptsachlich Informationen transportiert!

Ausgangslage (3)

Wer kommuniziert wie?

- Patienten, Mitarbeiter und Partner
- **E Mail** ist fester Bestandteil der Kommunikation und Wunsch der Mitarbeiter



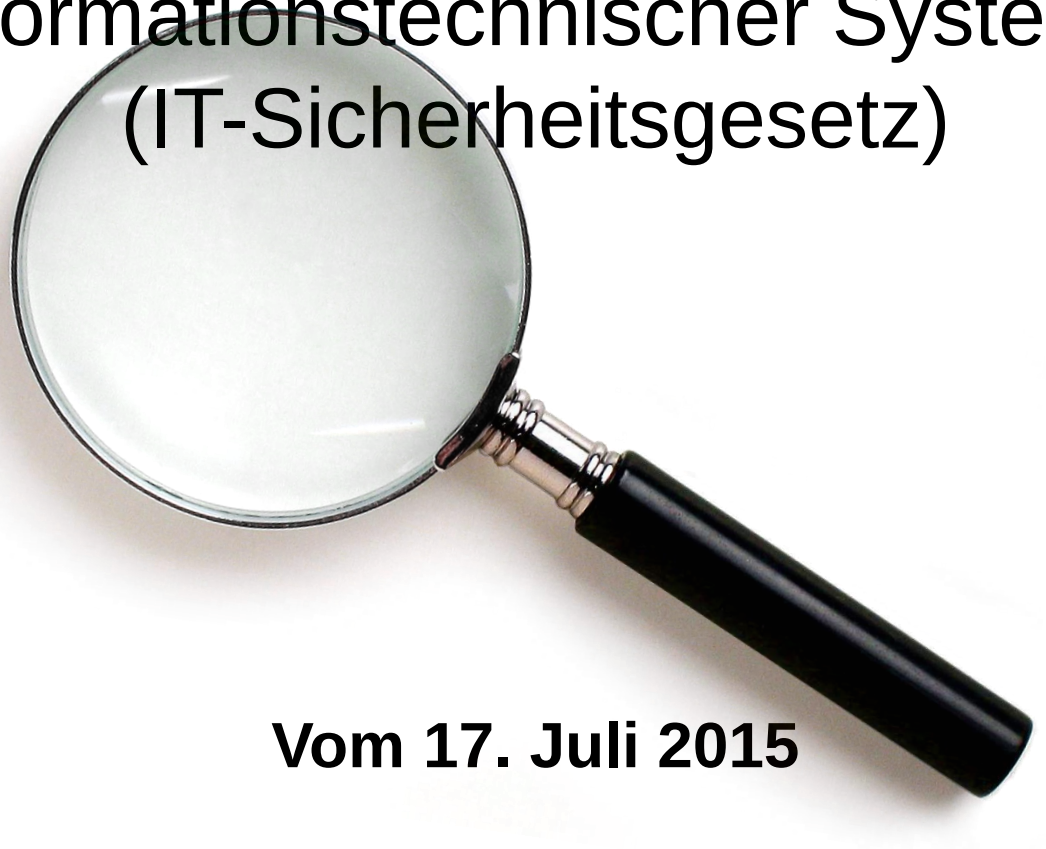
Ausgangslage (4)

Aber:

- Gefahrenbewußtsein bei E Mail ist äußerst gering
- Kein Mensch erfährt i.d.R, dass eine E Mail von **unberechtigten Dritten gelesen** wurden
- Maximal ein falscher Empfänger gibt Rückmeldung!
- Awareness fehlt !

Ausgangslage (5)

Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)



Vom 17. Juli 2015

Wen betrifft das IT-Sicherheitsgesetz?

- "Kritische Infrastrukturen (KRITIS) sind Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden."

Sektoren Kritischer Infrastrukturen	
Energie	Transport und Verkehr
Informationstechnik und Telekommunikation	Finanz- und Versicherungswesen
Gesundheit	Staat und Verwaltung
Wasser	Medien und Kultur
Ernährung	

Überblick

- über kbo
- Ausgangslage
- **Zieldefinition**
- Umsetzung
- Fazit

Zieldefinition

Ermittlung von E Mail Kommunikationspartnern

- intern & extern
- Art der ausgetauschten Daten (nach kbo Datenklassenmodell)
- Regelhaftigkeit der Kommunikation
- Kommunikationsweg (innerhalb AD / via Internet)

Auszug aus Analyse

Partner	Datenarten	Partner Infra-struktur	Häufigkeit	Schutzbedarf	Weg	Sicherheit
Konzernintern	Alle Arten von Daten	ok	stetig	hoch	Über eigenes AD in Citrix	In Ordnung
Vor- und Nachsorge	Med. Daten	mäßig	stetig	hoch	Internet / Fax	Keine sichere E-Mail
Patienten	Gesundheitsdaten	mäßig	Selten	hoch	Via Internet	Keine sichere E-Mail
Bewerber	Mitarbeiterdaten	mäßig	Selten	Mittel	Via Internet	o.k., upload

Exkurs Datenklassenmodell

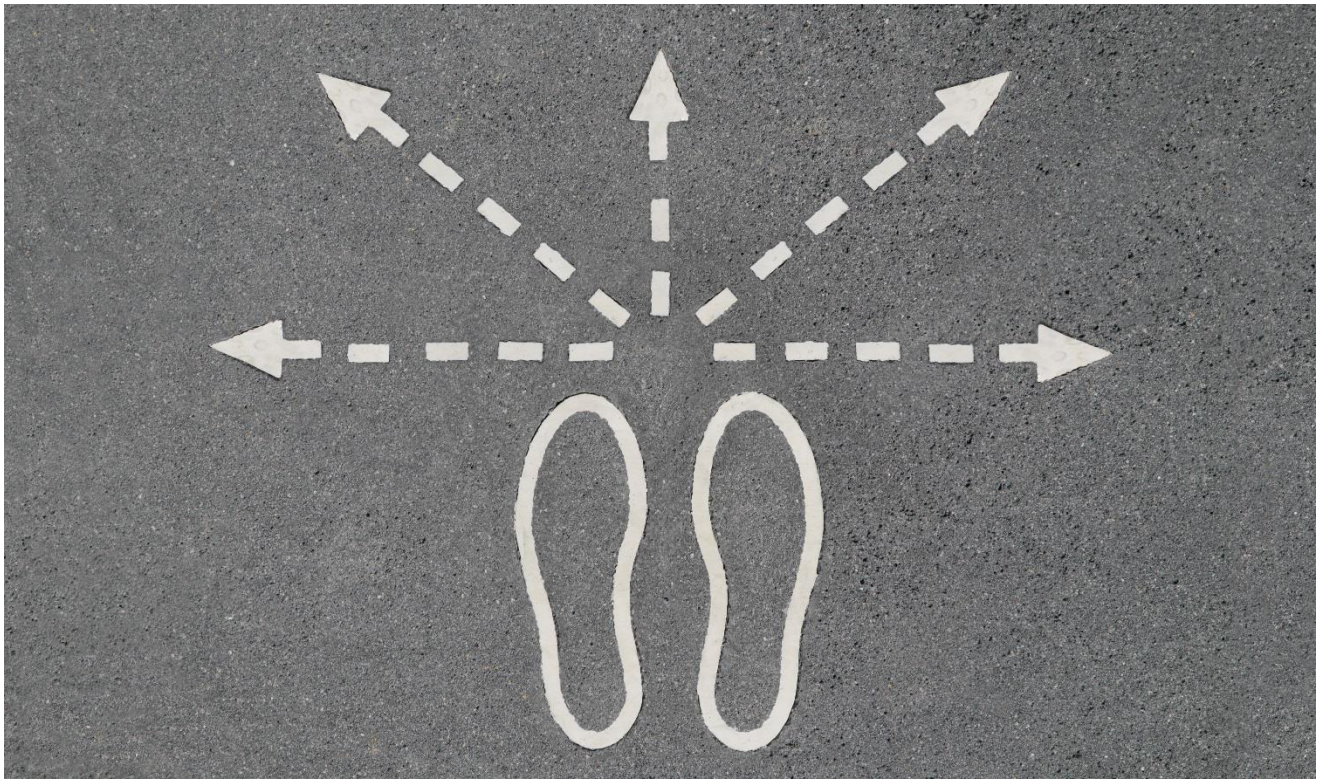
Es gibt 5 Datenklassen von 1 Med Daten bis 5 öffentliche Daten

	Datenklassen	Schutzbedarf	Zulässige Datenweitergabe	Daten Speicherung	Datenverfügbarkeit/ Wiederherstellung	Systemveränderung IT
1	**Medizinische Daten** z.B. Gendiagnostikdaten, Diagnosen, medizinische Gutachten, Untersuchungsergebnisse etc.	Hoher Schutzbedarf Ein Missbrauch der Daten kann das besondere Vertrauensverhältnis zwischen Arzt und Patient erheblich beeinträchtigen.	Klinikintern: – Daten aus Systemen: keine Weitergabe erforderlich, berechtigte Personen haben Zugriffsrechte. – Papierdokumente: an an der Behandlung beteiligte Personen per E-Mail unverschlüsselt, oder per Postweg in einem geschlossenen Umschlag, per Fax mit sofortiger Empfangsbestätigung des Empfängerberechtigten nach Extern: – Per E-Mail in verschlüsselter Form/Datei – Per Post – Per Fax mit sofortiger Empfangsbestätigung des Empfängerberechtigten – Datenträger (CD, USB) verschlüsselt und Passwortgeschützt per Post – Externe Zugriffe müssen über einen Vertrag zur Auftragsdatenverarbeitung abgesichert werden	• KIS-System und in Subsystemen wie z. B. OrgaCard, Labor, EEG etc. • Ambulanzsysteme • Patientenakte (Papier)	Störfallklasse 1	Entwicklung Kernsystem gemeinsam, lokale Änderungen über Schnittstellenanbindung zulässig Änderung über AK IT

Zieldefinition (2)

Festlegung:

- 2 Wege für sichere E Mail Kommunikation sind notwendig:



Zieldefinition (2)

Festlegung:

- 2 Wege für sichere E Mail Kommunikation sind notwendig:

  - **Weg 1**: ohne technischen Aufwand und mit niedriger Hemmschwelle
    - Anwender: Patienten, kleinste Versorgungspartner und einmalige Geschäftspartner

  - **Weg 2**: Austausch über sichere Systeme und ohne personellen Eingriff
    - Aufwand wie Zertifikatstausch im Vorfeld ist umsetzbar
    - Anwender: Große Partnerunternehmen wie Krankenhäuser, Wirtschaftsprüfer, Steuerberater etc.

Überblick

- über kbo
- Ausgangslage
- Zieldefinition
- **Umsetzung**
- Fazit

Umsetzung

Planung über mehrere Phasen

▪ Phase 1	✓ Bedarfserhebung und Kontakt mit den Partner ✓ Sensibilisierung der Führungskräfte ✓ Auswahl von geeigneten Möglichkeiten
▪ Phase 2	✓ Testlauf mit ausgewählten Benutzern zur Darstellung der Möglichkeiten
▪ Phase 3	✓ Roll Out der Verschlüsselung ohne technischen Aufwand ✓ Kommunikation mit den Anwendern ✓ Vorbereitung der IT für die Verschlüsselung über Server
▪ Phase 4	✓ Installation der Systeme für dauerhafte sichere Kommunikation ✓ Bereitstellung der Ressourcen und Ansprache der Partner
▪ Phase 5	✓ Einführung einer E-Mail Richtlinie für alle kbo Mitarbeiter

Umsetzung (2)

Aktuell befinden wir uns in der Phase 4

- Entscheidung für procilon Produkt proGOV und proTECTr
- Mehrere kurze Workshops zu Technik, Anwendung und Infrastruktur wurden durchgeführt
- Abstimmung des Stufenplans
- Erstellung einer kbo-eigenen proTECTr–Seite zur guten Akzeptanz
- proTECTr seit 2014 im Einsatz
- proGOV seit Mitte 2015 eingeführt

Überblick

- über kbo
- Ausgangslage
- Zieldefinition
- Umsetzung
- **Fazit**

Fazit

E-Mail Verschlüsselung ist unabdingbar

- Funktioniert - aber nur sofern
  - Notwendigkeit erkannt wird
  - der Partner eingebunden wird
  - Mitarbeiter keine Ängste vor der Nutzung haben
  - Technisch einfache Lösungen angeboten werden
  - organisatorische Regelungen mit berücksichtigt werden

- Hybrider Weg scheint zu funktionieren, da die Bandbreite der Anwendungsfälle abgedeckt werden kann

Branchenreferenz – Gesundheitswesen

Verschlüsselte Kommunikation bei den **Kliniken des Bezirks Oberbayern**

Das wurde erreicht:

- ✓ Einhaltung von **Compliance**
- ✓ **Geschäftsprozessoptierung**
- ✓ **Kosten- und Zeiteinsparung** durch verschlüsselten elektronischen Datenaustausch

REFERENZ Kliniken des Bezirks Oberbayern

Verschlüsselte Kommunikation mit proGOV und proTECTr

kbo

Zuverlässig an Ihrer Seite

Anwender

KBO - Kliniken des Bezirks Oberbayern

Branche

Gesundheitswesen

Herausforderung

Verschlüsselung des internen und externen E-Mailverkehrs zur Wahrung des Datenschutzes

Lösung

- proGOV
- proGOV Modul proTECTr
- proTECTr enterprise

Wichtige Daten zur richtigen Zeit am richtigen Ort

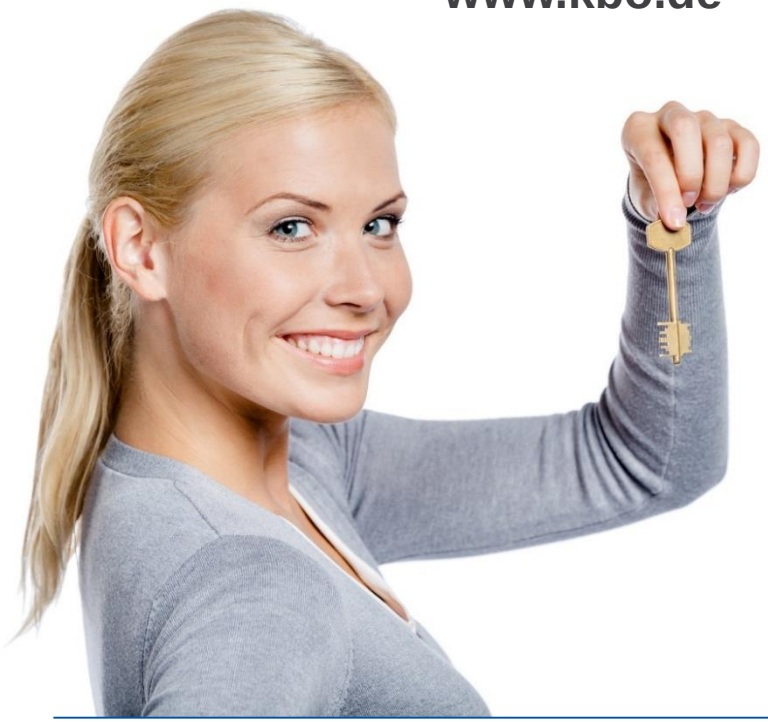
Kliniken sind aus Sicht der IT hochkomplexe Unternehmen. Ihre hohe Vernetzung auf Grund des stetigen Informationsflusses zwischen Patient, Arzt, Pflege, über Stationen, Gebäude und Organisationseinheiten hinweg, bedeuten für jede Klinik hohe logistische Herausforderungen.

Zentraler Bestandteil im Sinne der betriebswirtschaftlichen Unternehmensführung ist die Bereitstellung von Informationen zum richtigen Zeitpunkt an der richtigen Stelle über heute schon bestehende Kommunikationswege. Diese Grundanforderung hat zur Bildung heterogener IT-Landschaften, in welcher hauptsächlich Daten transportiert werden, beigetragen.

E-Mail ist ein fester Bestandteil der Kommu

als das beliebteste

Bleiben Sie sicher!



KBO – Kommunalunternehmen
Prinzregentenstraße 18, 80538 München
info@kbo.de
www.kbo.de

procilon GROUP
Leipziger Straße 110
04425 Taucha bei Leipzig

Londoner Bogen 4
44269 Dortmund

anfrage@procilon.de
www.procilon.de

procilon
GROUP
Signaturkarten
IT-Compliance
Sicherheitstechnologien
TR-ESOR
ePayment
neuerPersonalausweis
ElektronischeSignatur
E-Government-Gesetz
SichererDatenaustausch
Bürgerportale
Authentifizierung
EGVP-Integration
Signaturgesetz
Zugangseröffnung
1:1Marktkommunikation
XTA
Verschlüsselung
AS2
DINISO/IEC27001
IT-Sicherheit
nPA
OSCI
Risikoanalyse
PublicKeyInfrastructure
De-Mail
BSI-Grundschutz
VPS
Zertifikate
EGVP
Langzeitarchivierung
Beweiswerterhaltung
IT-Sicherheits-Analysen
TrustCenter
CloudServices
ErsetzendesScannen
ExternerDatenschutzbeauftragter
SSO
virtuellePoststelle
ElektronischerDatenaustausch
SigG
SingleSignOn
TR-RESISCAN