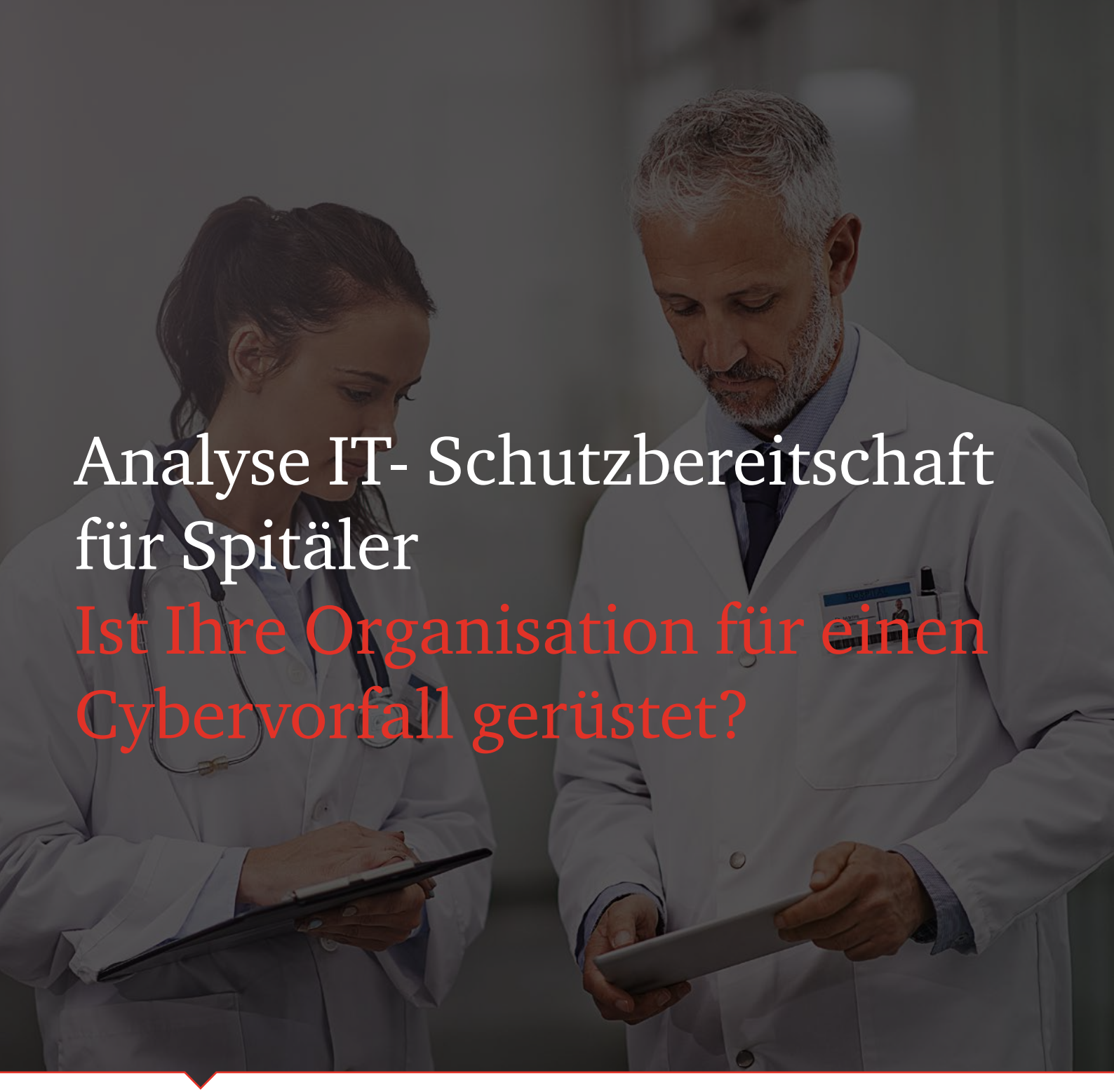


# Analyse IT- Schutzbereitschaft für Spitäler

## Ist Ihre Organisation für einen Cybervorfall gerüstet?

pwc

www.pwc.ch/cybersecurity

Die Digitalisierung schreitet voran – auch im Gesundheitswesen

## Die Digitalisierung erhöht die Abhängigkeit von IT

- In den letzten Jahren wurde das Gesundheitswesen zunehmend digitalisiert und vernetzt.
- Dieser Trend schliesst das elektronische Patientendossier und den damit verbundenen kontrollierten Austausch der elektronischen Patientendaten mit ein.
- Zusätzlich zur eigenen IT braucht es Schnittstellen mit Zuweisern, Leistungsträgern und anderen IT- und Businesspartnern.

## Personendaten müssen «angemessener» geschützt werden

- Gemäss eidgenössischem Datenschutzgesetz sind Gesundheitsdaten «besonders schützenswerte» Daten.
- Die eidgenössischen und kantonalen Gesetze verlangen einen «angemessenen Schutz der Daten» durch die Datenbearbeiter.
- Insbesondere werden angemessene technische und organisatorische Massnahmen und die Einschätzung der realistischen Risiken verlangt.

## Gesundheitswesen

Elektronische Daten helfen dabei, die Servicequalität im Spital zu verbessern, die Kosten zu senken und die Patienten effektiver zu behandeln. Daten sollen dort genutzt werden, wo sie benötigt werden. Verschiedene Spitäler hatten in den letzten Monaten überdurchschnittlich viel mit Malware zu kämpfen. Beispielsweise musste das Lukaskrankenhaus in Neuss (D) als Folge von Cyber-Malware sein Netzwerk vollständig herunterfahren – mit entsprechend grossem Einfluss auf den laufenden Betrieb. Als Konsequenz musste ein wesentlicher Teil der täglich rund 50 geplanten Operationen verschoben werden. (Februar 2016).

## IT-Security-Strategie und Governance

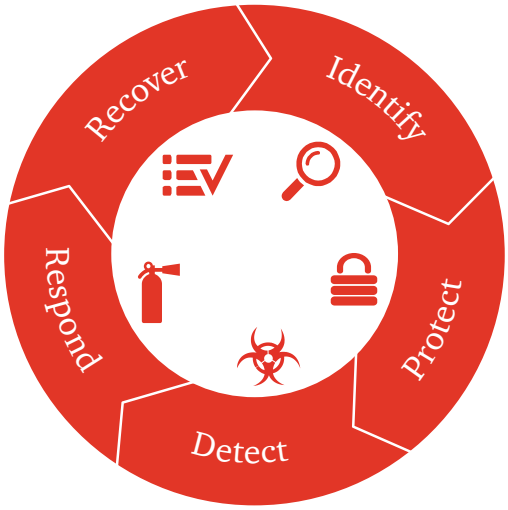
- Um sensitive Daten angemessen schützen zu können, muss man seine Daten kennen, das heisst, man muss sie identifizieren und klassifizieren.
- Wirksamer Datenschutz verlangt klar definierte Rollen und Zuständigkeiten. Zumindest die Rollen Data Owner, CISO, Information Security Officer und Compliance Officer müssen definiert und einer befähigten Person zugewiesen werden.
- Die technischen Sicherheitsmassnahmen sind keine «Selbstläufer». Es braucht genügend und geeignetes Betriebspersonal sowie Prozesse, um IT-Schutzmassnahmen gezielt umsetzen zu können (IT Security Operation).
- Gesetzliche und regulatorische Anforderungen müssen bekannt sein, damit sie eingehalten werden. Das regulatorische Audit verlangt dokumentierte Belege der Wirksamkeit von Schutzmassnahmen und Datenzugriffen (Nachvollziehbarkeit).

# IT Security – Referenz Architektur für das Gesundheitswesen

Die Frage ist heute nicht mehr, ob ein Spital Ziel eines Cyberangriffes wird, sondern nur noch wann. IT Security heute beinhaltet nicht nur Schutzmassnahmen (Protect), sondern auch die Fähigkeiten zum entdecken (Detect) und Reagieren (Respond) auf Cyber Angriffe. Somit braucht es die richtige Technologie, die richtigen Prozesse und Personalressourcen.

## Prozesse, Fähigkeiten, Ressourcen

Strategy




### Strategy
Aufbau, Steuerung und Aufsicht der Organisation. Managen von Geschäfts-Risiken und sicherstellen, dass Gesetze für die Bearbeitung elektronischen

### Identify
Verständnis für und Inventar von IT Assets, Daten und Prozesse sowie den Schnittstellen und Datenflüssen intern und extern.

### Protect
Massnahmen zum Schutz von sensitiven Daten und Information Assets vor Cyberbedrohungen und -angriffen. Limitierung des Schadensausmasses im Fall einer Kompromitierung.

### Detect
Erkennen von Sicherheitsvorfällen, Angriffen und Datenabflüssen. Einleiten von Gegenmassnahmen.

### Respond
Eingrenzung, Koordination und Triage der Massnahmen. Eskalation zum Krisen-mangement falls erforderlich.

### Recover
Bewältigen der Sicherheits-vorfälle und Rückkehr zum geordneten Betrieb sowie Minimierung der Auswirkungen für das Spital.

# Governance und Leadership

Welche Faktoren beeinflussen ihre Geschaäftsstrategie der nächsten 3-5 Jahre und was ist die Auswirkung auf die IT Security? Kennen Sie die Risiken und wie geht ihre Organisation damit um? Welche Bedrohungen wirken jetzt und in naher Zukunft auf ihre Organisation?


## Corporate Governance - IT / Security Governance

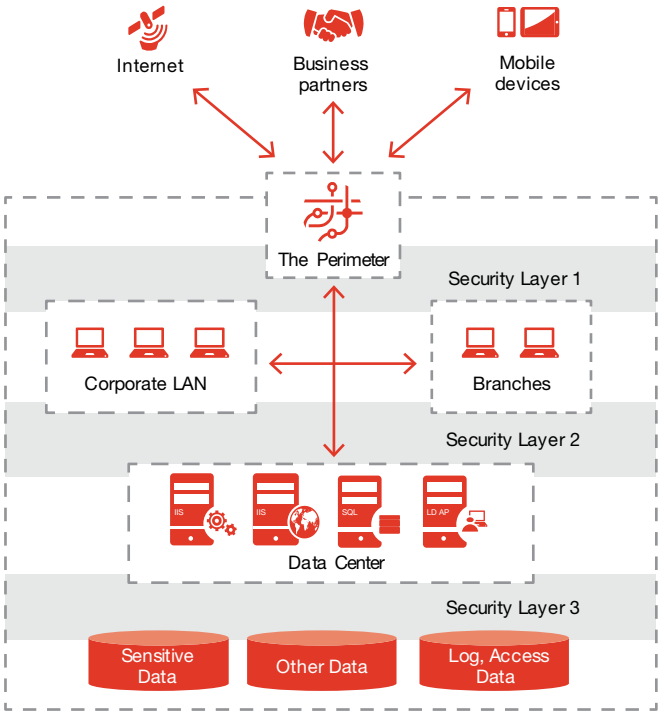
Dies umfasst die Gesamtheit der Grundsätze für die Leitung und Überwachung eines Unternehmens. Die IT ist mit den Geschäftsprozessen verzahnt. Dazu definiert der VR Ziele, Vorgehensweise, Rollen und Zuständigkeiten welche durch die GL kommunizieren und überwachen werden.

## Enterprise Risk Management - Cyber Risks

Enterprise Risk Management (ERM) ist ein ganzheitliches und unternehmensweites Risikomanagement und fasst unterschiedliche Sichtweisen wie Cyber-, Markt-, Währungs-, Technologie-, Operationelle Risiken mit ein.

## Compliance Management

Compliance-Management umfasst alle Massnahmen zur Sicherstellung der Compliance. Ziel des Compliance-Managements ist es, die Einhaltung von Gesetzen und Unternehmens-/ Konzernrichtlinien sicherzustellen und nachvollziehbar für eine Überprüfung zu dokumentieren.




## Schutz des Perimeter

Zugriffe von aussen und Datentransfers nach aussen müssen speziell überwacht werden (Partner Access, E-Mail, Remote Access, Guest WLAN).

## Transparenz aller IT Geräte im Netzwerk

Alle Geräte, die am Firmen-Netzwerk angeschlossen sind, müssen inventarisiert sein, und die Konfiguration sowie der Softwarestand muss geprüft werden.

## Monitoring für Nachvollziehbarkeit

Um Angriffe rechtzeitig erkennen zu können, braucht es eine stetige Analyse der Zugriffs-, Netzwerk- und Logdaten der Systeme und des Netzwerkverkehrs.

## Schutz des Zugriffs auf sensitive Daten

Personendaten sollen nur auf Systemen mit angemessenen Schutzmassnahmen gespeichert und bearbeitet werden. Zugriff auf Daten erhalten nur Policy-konforme Geräte von identifizierten Benutzer nach Need-to-do-/ Need-to-know-Prinzip.

# Was PwC für Sie tun kann: Analyse IT-Schutzbereitschaft im Spital

| Phase 1 | Phase 2 | | | | Phase 2 |
|---|---|---|---|---|---|
| Planung | Analyse und Benchmarking der Fähigkeiten, Prozesse und Ressourcen | | | | Report und Kommunikation |
| | Evidenzen | 1: Identifizieren | 2: Verifizieren | 3: Planen | |
| Ziel und Umfang festlegen<br><br>Schlüsselpersonen definieren<br><br>Dokumente zur Analyse identifizieren | Interview<br><br>Dokumenten-analyse<br><br>Prozessanalyse | Prozesse und Workflows verstehen<br><br>Schlüssel-personen befragen<br><br>Sicht auf Daten, Prozesse und Systeme anhand von 2–3 Workflows | Wirksamkeit der Sicherheits-massnahmen prüfen<br><br>Erkennen von Lücken und Verbesserungs-potenzial<br><br>Benchmark gegenüber Industry Good Practices | Priorisierung der nächsten Schritte zur Verbesserung der Cyber-security | Erstellen eines Reports und Diskussion mit Beteiligten<br><br>Präsentation gegenüber GL und VR (falls gewünscht) |

PwC hat eine speziell auf das Gesundheitswesen ausgerichtete Analyse entwickelt, um GL und VR in Spitälern die benötigte Klarheit darüber zu geben, ob ihre Organisation Datenschutzanforderungen erfüllt und vorbereitet ist, Cybervorfälle zu erkennen und zu beurteilen sowie diese effizient und effektiv zu bewältigen.

| Phase | Tätigkeit | Lieferobjekte |
|---|---|---|
| 1 | • Kick-off mit relevanten Schlüsselpersonen<br>• Abgrenzungen und Detailplanung | Detailplan des Assessments |
| 2 | • Identifizieren der Policies und Standards<br>• Auswahl von 3–5 Geschäftsprozessen, in denen sensitive Daten verarbeitet werden<br>• Erheben von Datenflüssen, Systemen und Sicherheitsmassnahmen<br>• Review, ob Daten entsprechend den Vorgaben und Industriestandards geschützt sind<br>• Gap-Analyse zwischen PwC-Referenz und aktueller Situation für Fähigkeiten, Ressourcen, Prozesse und Technologie | Benchmark für People, Prozesse und Technologie<br><br>Gap-Analyse:<br>• anwendbare Vorgaben<br>• Industriestandard |
| 3 | • Berichterstattung und Präsentation<br>• Priorisierung der Massnahmen | • Präsentation<br>• Bericht |

## Notwendige Schritte für eine stetige Verbesserung

1. Erstellen und Umsetzen einer IT und Security Strategie. Etablieren der IT und Security Governance durch das Identifizieren von schützenswerten IT Assets (Daten, IT Systeme Prozesse) und erstellen und pflegen eines Inventars.
2. Auswahl von relevanten Bedrohungsszenarien und Analyse der Auswirkungen von Sicherheitsvorfällen auf die Organisation in Bezug auf Verlust von Vertraulichkeit, Verfügbarkeit und Integrität von Daten sowie IT Systemen.
3. Überprüfung der implementierten Schutzmassnahmen (technisch und organisatorisch) auf deren Wirksamkeit und dem Erkennen von Schwachstellen.
4. Bewertung und Dokumentation der IT Security - and Technologie Risiken für jede Fachanwendung mit kontinuierlichem Risiko Management. Dies umfasst die Beurteilung der Risiken und wie damit umgegangen wird.
5. Schutzmassnahmen und Daten kontinuierlich überwachen durch befähigtes Personal. Wirksames Erkennen und Behandeln von Sicherheitsvorfällen. Stetiges Lernen aus den Sicherheitsvorfällen und erkennen von neuen Bedrohungen.

## Optionale Zusatzmodule:

| | | | | |
|---|---|---|---|---|
| «Game of Threat» – Simulation von Cyberangriffen für GL | Penetration Tests: (i) von aussen (ii) von innen, (iii) Social Engineering | Compromise Discovery Assessment unter Zuhilfenahme von Threat Intelligence | Rechtsberatung und Readiness Assement für Datenschutz und EU-GDPR | Cloud Readiness Assessment |

www.pwc.ch/cybersecurity

Reto Häni
Partner and Leader Cybersecurity
PwC Digital Services, Switzerland
+41 58 792 7512
reto.haeni@ch.pwc.com

Jean Paul Ballerini
Director Cybersecurity
PwC Digital Services, Switzerland
+41 58 792 2697
jean.paul.ballerini@ch.pwc.com

Urs Küderli
Director Cybersecurity Strategy and Transformation
PwC Digital Services, Switzerland
+41 58 792 4221
urs.kuederli@ch.pwc.com

Lorenz Neher
Senior Manager Cybersecurity Security Technology
PwC Digital Services, Switzerland
+41 58 792 4785
lorenz.neher@ch.pwc.com