Informationssicherheit im Spital

Realität oder Wunschdenken?

Kantonsspital Graubünden

Inhalt

- Wie steht es um die Informationssicherheit in Schweizer Spitäler? (20’)
- Weshalb klappt es nicht? (10’)
- Und was können wir nun tun? (10’)
- Q&A (5’)

Kantonsspital Graubünden

Zu meiner Person

Stefan Juon, Co-Leiter ICT und CISO am Kantonsspital Graubünden

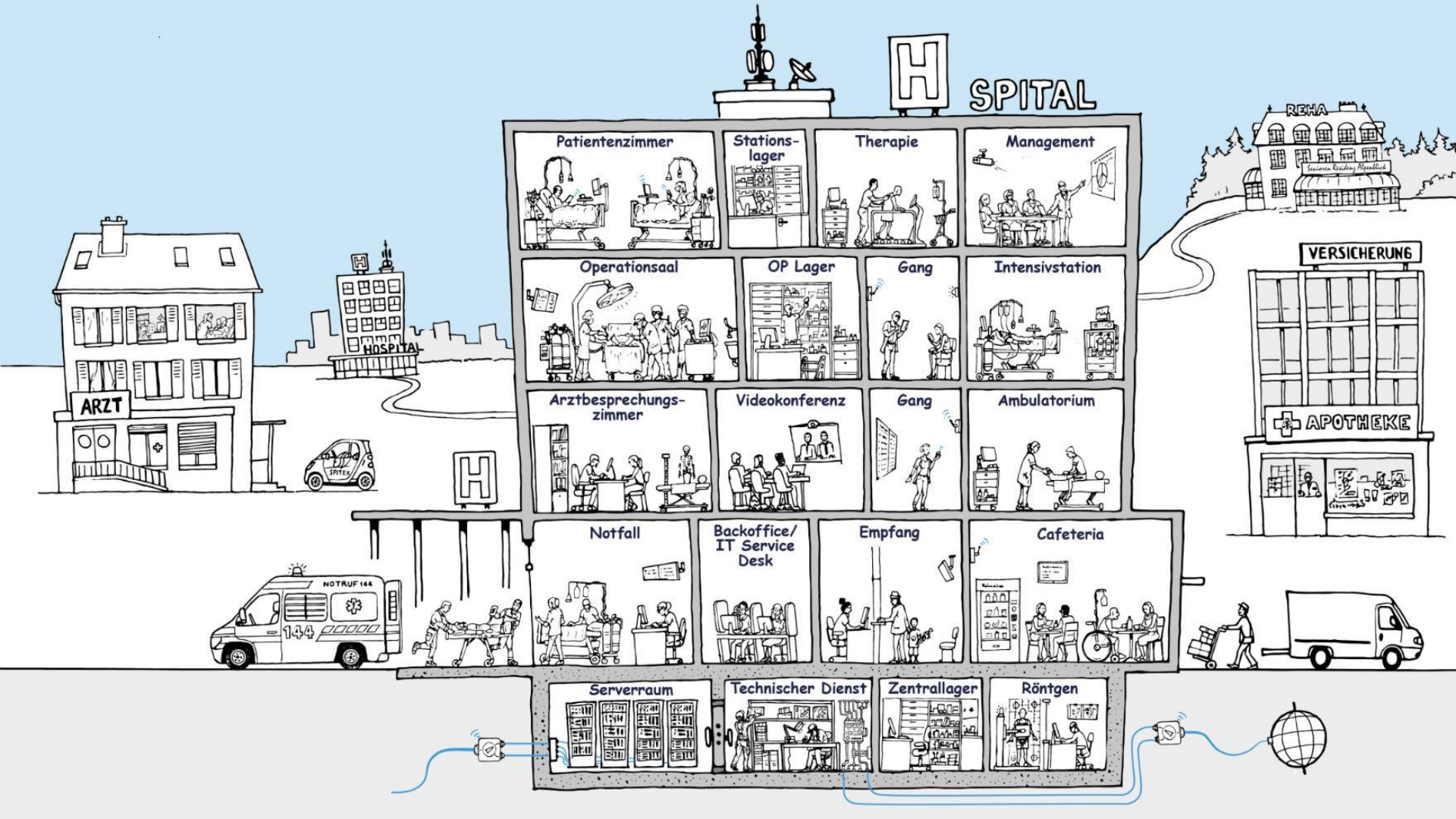
seit 2009 am Kantonsspital Graubünden tätig, seit 2016 in der Rolle als CISO verantwortlich für die Informationssicherheit am KSGR

stefan.juon@ksgr.ch

Kantonsspital Graubünden

Wie steht es um die **Informationssicherheit** in Schweizer Spitäler?

Kantonsspital Graubünden


H SPITAL
Patientenzimmer
Stations-lager
Therapie
Management
Operationsaal
OP Lager
Gang
Intensivstation
Arztbesprechungs-zimmer
Videokonferenz
Gang
Ambulatorium
Notfall
Backoffice/ IT Service Desk
Empfang
Cafeteria
Serverraum
Technischer Dienst
Zentrallager
Röntgen
REHA
VERSICHERUNG
APOTHEKE
ARZT
HOSPITAL
NOTRUF 144
144

Schutzziele der Informationssicherheit

Vertraulichkeit, Integrität und Verfügbarkeit

Erweiterte Schutzziele:

- Nichtabstreitbarkeit
- Authentizität
- Verlässlichkeit

Schutzziele der Informationssicherheit

Vertraulichkeit, Integrität und Verfügbarkeit

Vertraulichkeit

Integrität

Verfügbarkeit

Schutzziel Vertraulichkeit

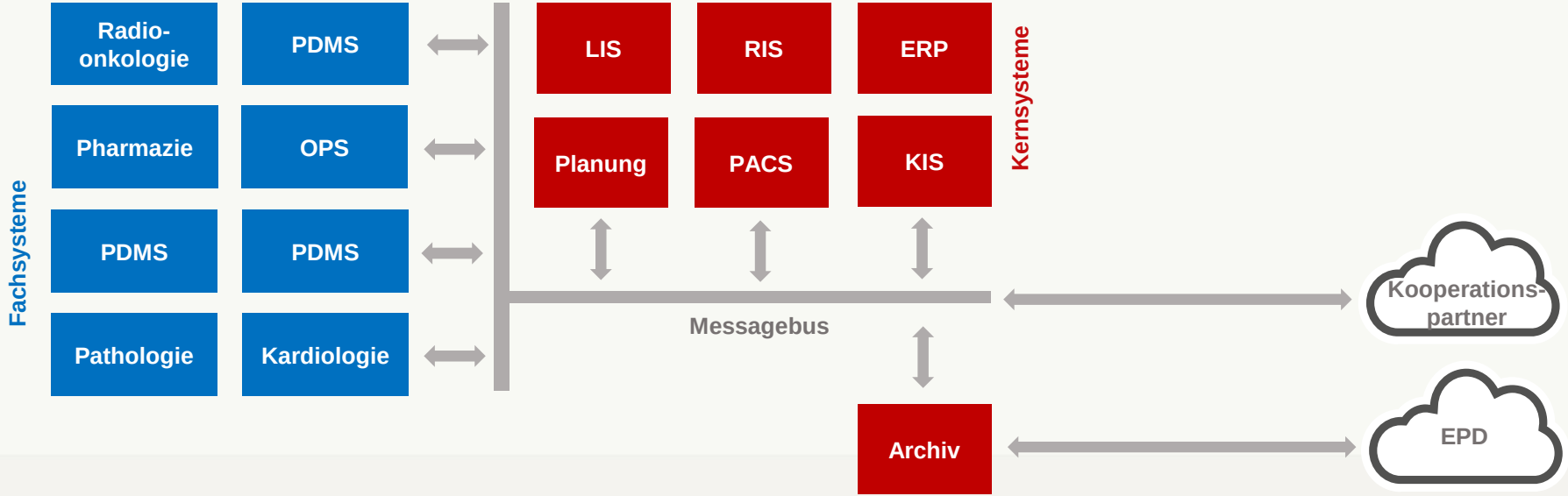
Feststellungen

- Das Grundverständnis im Spitalumfeld zur Vertraulichkeit von Patientendaten ist per se vorhanden.
- Die dezentrale Haltung von Patientendaten in zahlreichen Informationssystemen erschwert die effiziente Durchsetzung von Massnahmen.
- Eine grosse Herausforderung ist eine konforme Umsetzung von Zugriffsberechtigungen in Kern- und Fachsystemen.
- Die vertrauliche Kommunikation mit dem Patienten ist ungelöst.

Kantonsspital
Graubünden

Fokus dezentrale Datenhaltung

Weshalb dezentrale Datenhaltung eine Herausforderung ist



Kantonsspital Graubünden

Fokus dezentrale Datenhaltung

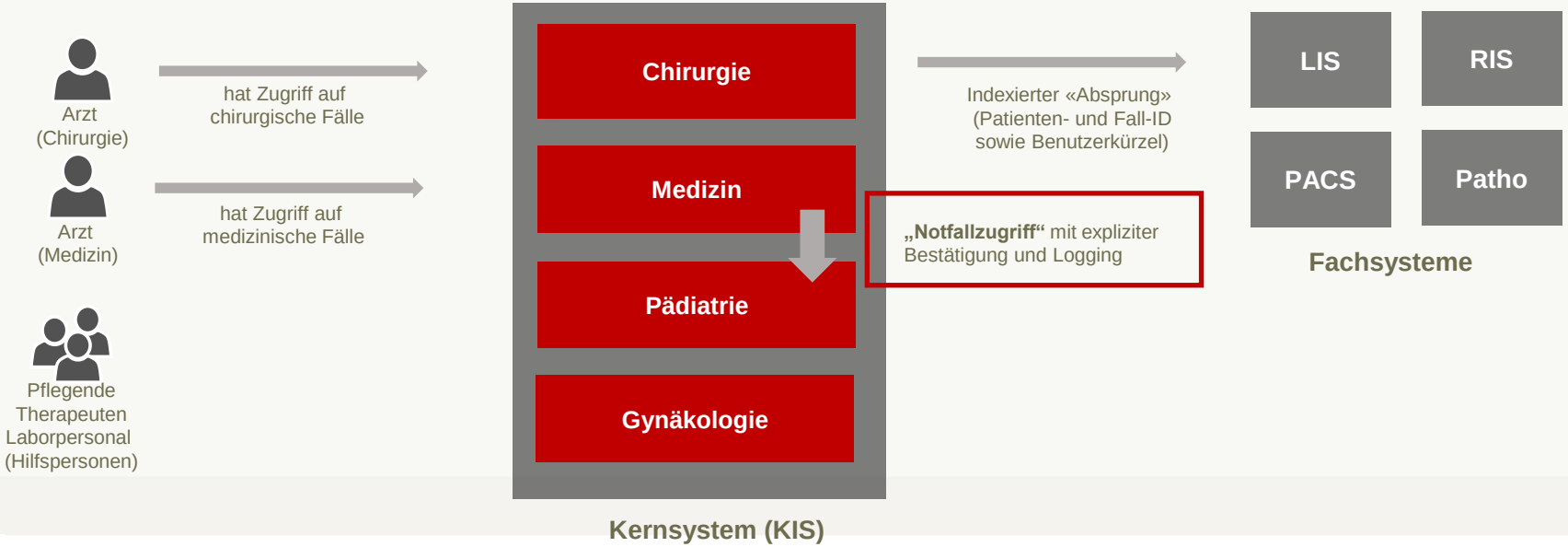
Schutzziel Vertraulichkeit

- Die einheitliche Umsetzung und Kontrolle von Massnahmen in einer Systemlandschaft mit dezentraler Datenhaltung ist anspruchsvoll.
- Als Beispiel: Eine Vorgabe zur verschlüsselten Datenspeicherung erfordert auf einem datenbankgestützten Informationssystem eine andere Umsetzung als auch einem dateigestützten System.
- Daraus folgend gilt es zu akzeptieren, dass in einem solchen Setting die 100% kaum erreichbar sein werden und ergo ein Gap bestehen bleibt.

Kantonsspital Graubünden

Fokus Zugriffsberechtigungen

Zugriffsberechtigungen im KIS am KSGR



Kantonsspital Graubünden

Fokus Zugriffsberechtigungen

Wie sie optimal zu regeln wären

- Nach Art. 321 StGB ist die Offenbarung von Geheimnissen, welches Ärzten sowie ihren Hilfspersonen infolge ihres Berufes anvertraut worden ist oder das sie in dessen Ausübung wahrgenommen haben, strafbar.
- Die Zugriffsberechtigungen in medizinischen Informationssystemen sollten nach diesem Grundsatz ausgerichtet sein. Das bedeutet konkret, dass Zugriffe auf einen Datensatz beim Verfasser beantragt und von diesem gewährt werden müssen.

Kantonsspital Graubünden

Schutzziel Vertraulichkeit

Was uns zu Denken geben muss – aktuelle Tendenzen

- Die Gefährdung der Cyberkriminalität hat sich auf hohem Niveau etabliert und wird sich weiter akzentuieren.
- Die Anzahl an Schwachstellen in Services und Applikationen bleibt hoch. Davon gefeit ist nichts und niemand. Dies ist als Realität und nicht als Hypothese zu verstehen.
- Das EPD in der jetzigen Form löst die vertrauliche Kommunikation mit dem Patienten nur teilweise.
- Passwortdatenbanken, welche im Darknet käuflich angeboten werden und sich durch Data-Breaches speisen, haben immense Grössen angenommen.

Wie steht es um die Informationssicherheit in Schweizer Spitäler?

Zwischenstand 1/3

Vertraulichkeit

Integrität

Verfügbarkeit

Kantonsspital Graubünden

Schutzziel Integrität

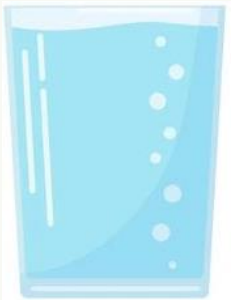
Feststellungen

- Die in klinischen Informationssystemen gespeicherten Patientendaten sind in aller der Regel nicht signiert und somit anfällig auf Manipulation. Aber: Sofern die Systeme ausreichend system- und zugriffsgeschützt sind kann dieses Risiko akzeptiert werden.
- Die Nachvollziehbarkeit (Non-Repudation) von Manipulationen von Datensätzen fehlt in zahlreichen Informationssystemen.

Wie steht es um die Informationssicherheit in Schweizer Spitäler?

Zwischenstand 2/3

Vertraulichkeit



Integrität

Verfügbarkeit

Kantonsspital Graubünden

Schutzziel Verfügbarkeit

Feststellungen

- Es existieren ausreichend Technologien, um informationsverarbeitende Systeme verfügbar bereitzustellen.
- Die anhaltende Gefährdung durch Ransomware beeinträchtigt das Schutzziel der Verfügbarkeit wesentlich.
- Die Fortführung des Geschäftsgangs (Business Continuity) ist unzureichend geregelt. Es fehlt teilweise an einfachsten Impact Analysen und nicht zuletzt an der Einsicht der Notwendigkeit.

Fokus Notfallmanagement

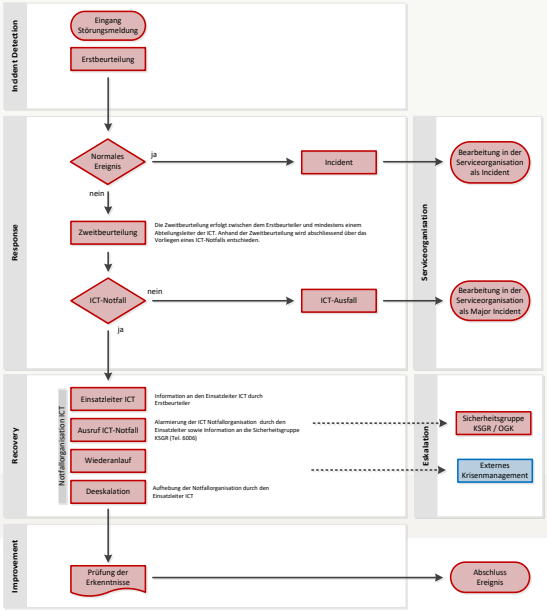
Bestandteile eines ICT Notfallmanagements

Rollen:
- Einsatzleiter ICT
- Technischer Leiter ICT
- Leiter Supportteam
- ICT Notfallteam
- ICT Team

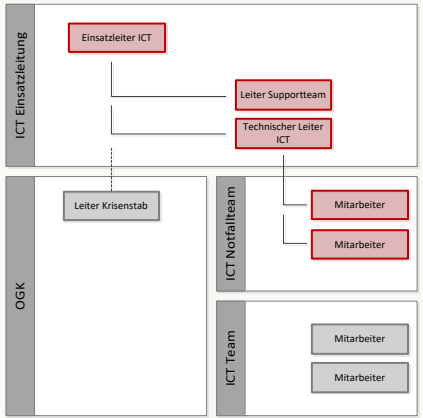
Stabsarbeit:
- **F** (Facts)
- **O** (Options)
- **R** (Risks & Benefits)
- **D** (Decision)
- **E** (Execution)
- **C** (Check)

Normen:
- ISO/IEC 27031:2011

Prozesse:



Organisation:

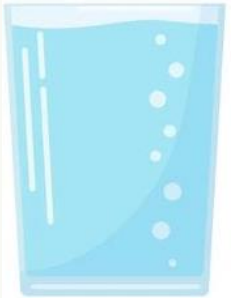


Kantonsspital Graubünden

Wie steht es um die Informationssicherheit in Schweizer Spitäler?

Schlussstand

Vertraulichkeit



Integrität

Verfügbarkeit

Kantonsspital Graubünden

Warum klappt es nicht?

Kantonsspital
Graubünden

Warum klappt es nicht?

Thesen (1/2)

- Die Budgets für ICT und Informationssicherheit sind zwar steigend, in der Gesundheitsbranche im Vergleich mit anderen Branchen aber weiterhin tief (gilt ebenso für Digitalisierungsvorhaben).
- Es fehlt an verpflichtenden Minimalvorgaben innerhalb der Branche, welche an die Betriebserlaubnis geknüpft sind.
- Interne Revisionen finden kaum oder gar nicht statt.

Warum klappt es nicht?

Thesen (2/2)

- Die Risiken der Cybercrime werden noch nicht durchgängig als Unternehmensrisiken verstanden und behandelt.
- Die ausgesprochen hohe Anzahl an Applikationen in einem Spital erschweren zentrale Massnahmen.
- Das Schutzziel der Verfügbarkeit von Daten steht über dem Schutzziel der Vertraulichkeit und schwächt dieses teilweise. Patientendaten müssen immer verfügbar und zugreifbar sein, damit die Behandlung auch im Notfall erfolgen kann. Die Vertraulichkeit muss dabei manchmal „hinten anstehen“.

Kantonsspital Graubünden

Und **was** können wir nun tun?

Kantonsspital
Graubünden

Wer ist verantwortlich?

Interpellation 17.3136 von Bea Heim vom 15.3.2017

17.3136 INTERPELLATION

Cybersicherheit im Gesundheitswesen

Eingereicht von:	 HEIM BEA Sozialdemokratische Fraktion Sozialdemokratische Partei der Schweiz
Einreichungsdatum:	15.03.2017
Eingereicht im	Nationalrat
Stand der Beratungen:	Im Rat noch nicht behandelt

https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173136

Kantonsspital Graubünden

Wer ist verantwortlich?

Antwort vom Bundesrat vom 10. Mai 2017 [1)]

- «Jedes Unternehmen ist für den sicheren Betrieb seiner IT-Infrastruktur selber verantwortlich.»
- «Die Verantwortung und damit auch die Haftung für die Sicherheit eines Medizinproduktes liegen beim Hersteller.»

Quelle: https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173136

[1)] Zwei Tage später hat die Welt mit WannaCry den bisher verheerendsten Cyberangriff gesehen.

Was ist zu tun?

10 konkrete Handlungsempfehlungen (1/4)

1. Verstehen und behandeln Sie Cyberrisiken als Unternehmensrisiken. Verwalten Sie Ihre IT- und Cyberrisiken und richten Sie Ihre Massnahmen danach aus.
2. Schützen Sie sich gegenüber Ransomware. Betreiben Sie ein diszipliniertes Patchmanagement, sichern Sie Ihre Fernzugänge und ins Internet exponierten Dienste ab, blockieren Sie suspekte E-Mails und widmen Sie der Datensicherung hohe Aufmerksamkeit.

Was ist zu tun?

10 konkrete Handlungsempfehlungen (2/4)

3. Zonieren Sie Ihre Netzwerke, definieren Sie Abwehrlinien und passen Sie diese regelmässig an. Setzen Sie ein Defense-in-Depth Konzept um.
4. Kümmern Sie sich um Ihre Zugriffsberechtigungen und investieren Sie in griffige Zugriffskonzepte sowie Nachvollziehbarkeit von Zugriffen. Trennen Sie administrative von nicht-administrativen Zugriffsberechtigungen innerhalb der ICT (Segregation of Duties).
5. Schaffen Sie Visibilität über die Aktivitäten in Ihrem Netzwerk. Legen Sie ein besonderes Augenmerk auf die User and Entity Behavior Analytics (UEBA). Setzen Sie dazu ein SIEM oder vergleichbare Technologien ein.

Was ist zu tun?

10 konkrete Handlungsempfehlungen (3/4)

6. Nutzen Sie Frameworks (ISO27000, BSI Grundschutz und NIST Cybersecurity Framework Core).
7. Gehen Sie davon aus, dass Sie von einem Ereignis betroffen sein werden. Investieren Sie deshalb in die Reaktion. Definieren Sie zumindest ein Notfallmanagement für die ICT und schaffen Sie „Forensic Readyness“. Zentralisieren Sie dazu die Protokollierungen von Systemen und Applikationen und schützen Sie diese adäquat.
8. Penetrationtestings alleine reichen nicht mehr aus. Führen Sie ergänzend ein Red Teaming durch.

Kantonsspital Graubünden

Was ist zu tun?

10 konkrete Handlungsempfehlungen (4/4)

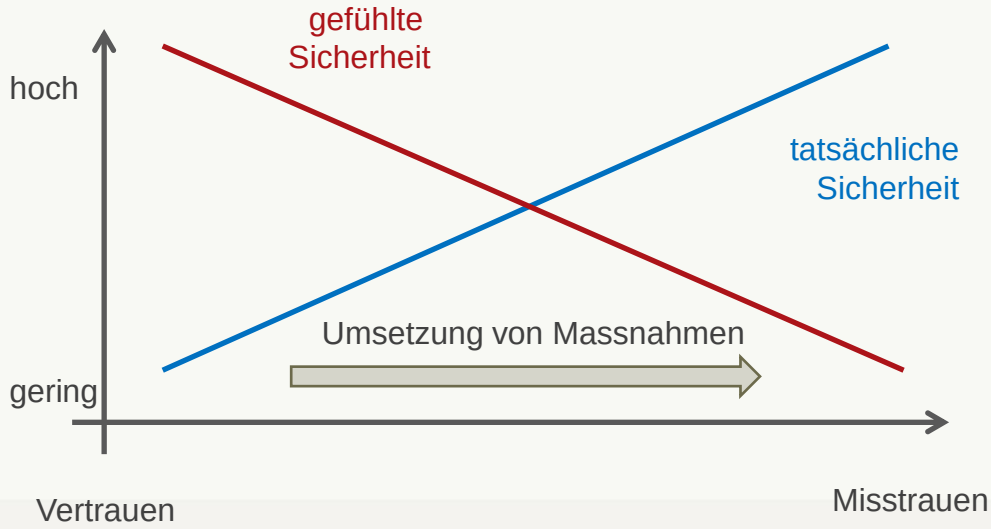
9. Halten Sie Ihr Asset-Management stets aktuell. Verstehen Sie nicht nur Systeme und Applikationen als Assets, sondern ebenfalls Ihre Lieferanten, Verträge etc.

10. Verwalten Sie Ihre Lieferanten und Dienstleister aktiv. Legen Sie auch ein besonderes Augenmerk auf die Fernzugriffe Ihrer Lieferanten. Wenden Sie strikte Authentisierungs-Vorgaben an und zeichnen Sie die Zugriffe auf.

Behalten Sie Augenmass

Wieviel ist zu viel?

"Der Mensch sehnt sich nach Vertrauen und hat eine instinktive Ablehnung gegen Massnahmen, die Misstrauen ausdrücken. Das Gefühl des Vertrauens wird als freundlich und sicher empfunden. In einer feindlichen Umgebung, in der es an Vertrauen fehlt, fühlt man sich unsicher und ausgesetzt. Die gefühlte Sicherheit verläuft genau entgegen der tat-sächlichen Sicherheit."



Quelle: Konfliktmanagement für Sicherheitsprofis
Sebastian Klipper
ISBN 978-3-8348-1686-3

Kantonsspital Graubünden

Herzlichen Dank
für Ihre Aufmerksamkeit.

Kantonsspital
Graubünden