# Die Sorgen eines CISO, Herausforderungen und Lösungsansätze

Miloš Božović, 8. September 2014
Klassifikation: C1

swisscom

# Zitat





> Wer wesentliche Freiheit aufgeben kann um eine geringfügige bloß jeweilige Sicherheit zu bewirken, verdient weder Freiheit, noch Sicherheit.
>
> Benjamin Franklin

# Inhalt

# Über den Präsentierenden





- Miloš Božović
- Arbeitet in Zürich, siehe Foto
- Bei Swisscom seit 2013, zuvor bei Bank Julius Bär, PricewaterhouseCoopers und Siemens tätig

- Warum verrate ich Ihnen so viel? Hören Sie sich die Idee von Swisscom an.

# Was Informationssicherheit ist

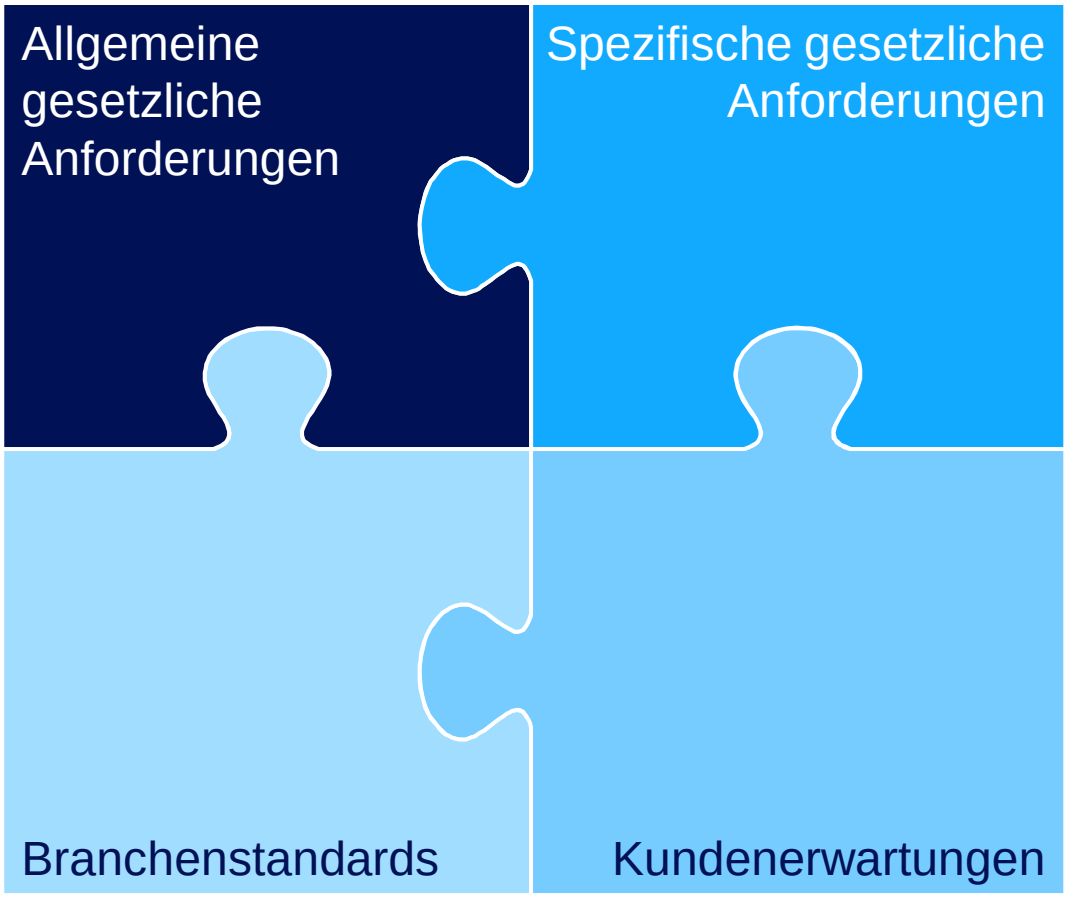




- Informationssicherheit befasst sich mit dem Schutz vor Gefahren und Bedrohungen sowie der Vermeidung von Schäden und der Minimierung von Risiken.
- Verschiedene Aspekte der Informationssicherheit:
  - Confidentiality (Vertraulichkeit)
  - Integrity (Integrität)
  - Availabilty (Verfügbarkeit)
- Weitere wie non-repudiation (Nichtabstreitbarkeit), Business Continuity und andere gibt es ebenfalls, aber wir konzentrieren uns auf die erstgenannten.

# Warum wir uns damit befassen





# Herausforderungen eines CISO





- Management verschiedener Partner; expectaction management
- Betriebsprozesse müssen funktionieren
- Die damit verarbeitete Information muss, wo notwendig, geschützt sein
- Ansprüche entstehen von allen Seiten
  - Management
  - Betrieb
  - Belegschaft
  - Kunden
  - Gesetzgeber
  - Lieferanten
  - Veränderungen technischer und organisatorischer Natur

# Was besonders im Gesundheitswesen ist





- Es geht um Menschenleben, nicht nur um Waren oder Geld
  - Lebenserhaltende Geräte sind heute vernetzt, selten geschützt
- Sicherheit ist zwar wichtig, aber funktionierende Prozesse sind wichtiger
  - Die Einlieferung in den OP muss schnell sein und funktionieren!
- Krankenhäuser sind in erster Linie für alle offen
  - Man kann ohne Weiteres in den Notfallbereich reinlaufen
- Aber damit kommt auch jeder fast überall rein
  - Social Engineering als Methode ist einfach anwendbar
- Lohnenswerte Ziele weil viele Informationen über Patienten vorhanden:
  - Oftmals werden die Daten für wirtschaftliche Kriminalität gebraucht
  - Vorbereitung weiterer Angriffe wird erleichtert
  - Störung von Spitälern kann auch bei konventionellen Angriffen helfen

# Analogie: Flughafen





## In Nordamerika

- Stufenweise Sicherheit, aber starke Konzentration
- Polizeipatrouillen am Flughafen, Abschreckung
- Grosse Sicherheitspräsenz bei Kontrollen und rund um die Flugzeuge
- Im Notfall ist eine Räumung des Flughafens geplant → geht sehr lange

## In Israel

- Stufenweise Sicherheit, verteilt
- Unauffällige Prüfung am Parkplatz
- Unauffällige Prüfung vor dem Flughafengebäude
- Unauffällige Prüfung am Check-In Schalter
- Sicherheitskontrolle
- Im Notfall keine Räumung nötig → Sicherheitsraum

**Man setzt eher auf Schulung als auf Abschreckung**

# Mögliche Lösungansätze





- Eine Sicherheitskultur pflegen: Der einzelne Mitarbeiter sorgt am besten für Sicherheit
- Datensparsamkeit: Nur notwendige Informationen sollen gespeichert oder übertragen werden
- Die Mitarbeiter prüfen: Vertrauenswürdige Mitarbeiter dürfen eher mit heiklen Daten arbeiten
- Mitarbeiter schulen: Ob umfassende Schulungen oder Flyer mit Stichworten, Sicherheit fängt beim Mitarbeiter an
- Setzen Sie Massnahmen um: Wo notwendig, sollen herkömmliche Sicherheitsmassnahmen eingesetzt werden
- Massvolle Erneuerung: Neue Technologien sind gut, wenn sie sinnvoll eingesetzt werden
- Verwalten Sie Ihr Inventar: (Mobile) Geräte sollen zentral gesteuert werden

# Mögliche Lösungansätze





- Kopieren Sie die anderen: Alle haben ähnliche Probleme
- Sicherheit wird rundherum gebaut: Hohe Mauern auf einer Seite und keine auf der Rückseite ist auch keine Lösung

# Wie es Swisscom macht



> Wir pflegen eine offene, vertrauensvolle Kultur, in welcher wir Informationen dort verfügbar machen wollen, wo sie sein müssen.

Roger Halbheer, CISO Swisscom AG



swisscom

# Wie es Swisscom macht





> Wir erlauben den Zugriff von allen möglichen Computern aus
> Geräte und Software, die wir herstellen, prüfen wir
> Wir erlauben den Zugriff von überall her
> Der Zugriff läuft Browser-basiert ab
> Die Daten, die abgerufen werden, sind C1 oder C2 klassifiziert
> Wir schulen die Mitarbeiter
> Wir vertrauen den Mitarbeitern
> Wir machen «Human Centered Security»

> Trotz allem wird es auch bei uns Lücken geben.

Totale Sicherheit gibt es nicht!

# Erkenntnisse





- Sicherheit fängt beim Mitarbeiter an
- Sicherheit lässt sich am besten umsetzen, wenn alle mitmachen
- Sicherheit lässt sich schulen
- Sicherheit ist nicht immer ein «Hinderungsfaktor»
- Sicherheit ist dann effektiv, wenn sie am richtigen Ort ansetzt
- Sicherheit sollte einfach verpackt werden, um verstanden zu werden
- Ganz ohne Sicherheit geht es meist nicht (Gesetze…)

# Abschluss





- Warum habe ich Ihnen nun anfänglich «so viel» über mich verraten?
- Diese Informationen sind frei verfügbar, C1 klassifiziert und mit einer einfachen Internetrecherche ohnehin auffindbar.
- Finde ich ebenfalls gleich viel über Sie heraus? Vermutlich schon. Was lehrt uns das?
  - Datensparsamkeit! In allen Ausprägungen.

# Fragen und Antworten





> Bitte stellen Sie Ihre Fragen.

> Falls später Fragen auftauchen, können Sie mich gerne kontaktieren.

> Wenn Sie in Zürich sind, kommen Sie auf einen Kaffe vorbei!

# Kontakt



Swisscom AG

Miloš Božović
Group Security
Hardturmstrasse 3
8005 Zürich

Phone +41 58 224 14 58
milos.bozovic@swisscom.ch
www.swisscom.ch





swisscom

# Zusatzinformationen





> Anbei eine kleine Ansammlung von interessanten Quellen:
  - ISO 2700x Standard: http://de.wikipedia.org/wiki/ISO/IEC_27000-Reihe
  - HL7 Standard: http://de.wikipedia.org/wiki/HL7
  - HIPAA Title II: http://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act
  - EN 60601 Standard: http://de.wikipedia.org/wiki/EN_60601