

- » Schützen Sie Daten?
- » Spionage ist normal
- » Sicher mit Roadmap
- » Angriffe abwehren
- » Angst vor der Cloud?

## Sehr geehrte Damen und Herren,

---

Die Digitale Transformation durchdringt alle Wirtschaftsbereiche: Von Gesundheitswesen über Finanzindustrie und Energiesektor bis hin zu Medien – alle sind von der Digitalisierung betroffen. Im digitalen Zeitalter sind Daten das neue Gold. Dementsprechend hart umkämpft und auch reguliert sind sie heute.



Doch im Zeitalter von Big Data müssen sich Daten jeglichen Umfangs unkompliziert und zuverlässig austauschen lassen. Der Austausch sicherer Daten funktioniert aber nur, wenn bestimmte Schutzmassnahmen gegeben sind. Auch darum müssen Sicherheit und Business-Software für Schweizer CIOs dieses Jahr höchste Priorität haben.

Wie steht's bei Ihnen?

Roger Eric Gisi



---

## DIGITALE TRANSFORMATION

---



### Ein neuer Touchpoint für die digitale Transformation

---

Digitaler Wohlstand, Digitale Wirtschaft, Digitales Leben – ist dies tatsächlich der Stoff, aus dem die Zukunft gewebt wird? [Digitale Schweiz – Initiative für »Smart Switzerland«](#)

---

## SICHERHEIT WELT

---



### Schützen Sie Daten?

---

2018 sollen die [neuen EU-Datenschutzbestimmungen](#) in Kraft treten. Für Unternehmen jeder Grösse, die Daten sammeln, speichern und verarbeiten, bringt dies eine höhere Verantwortung für die Datensicherheit und umfangreichere Rechenschaftspflichten mit sich. Gehen Sie aktiv vor und schützen Sie Ihre Daten – und Ihr Kapital. Bei Verstössen drohen massive Bussen.

### Putin kritisiert Nato

---

Der russische Präsident Putin hat den Aufbau des [Nato-Raketenschutzschirms](#) als weltweite Bedrohung kritisiert. Russland müsse sich der «Bedrohung seiner Sicherheit» stellen. Einen neuen Rüstungswettlauf mit den USA will Putin aber nicht in Kauf nehmen. «Wir werden alles Nötige tun, um das strategische Gleichgewicht zu wahren», sagte Putin.



### Spionage ist normal

---

Der Nachrichtendienst des Bundes (NDB) hat seinen Lagebericht «Sicherheit Schweiz» für das Jahr 2016 veröffentlicht. Neben den Krisenherden in Nahost und Russland, geht es darin auch um Wirtschaftsspionage und wie Schweizer Firmen mit Cyber-Mitteln ausgehorcht werden. Laut NDB ist Spionage bei uns ist üblich. Im letzten Jahr hat sie sogar markant zugenommen.



### Rechts gewinnt

---

Was die letzten Wahlen gezeigt haben, bestätigt ein aktueller Bericht des Forschungsinstituts GfS Bern: In der Schweiz geht ein Wertewandel vonstatten. Dabei gewinnen bürgerliche Haltungen an Rückhalt. Der Studie zufolge hat in den letzten Jahren vor allem das Sicherheitsbedürfnis zugenommen, was die Forscher auf den islamitischen Terror zurückführen.

---

## RISIKO-MANAGEMENT

---



### Times Change!

---

Why would cyber criminals attack small and medium enterprises (SME)? It's often thought that they only target financial institutions and large multinationals. Not anymore: According to [«The Global State of Information Security Survey 2016»](#), the financial costs of security incidents have increased by 100% for SMEs, while those for large organizations have fallen by 20%.



### Sicher mit Roadmap

---

Die Digitalisierung macht es schwierig, geschäftliche Daten und Anwendungen vor unbefugtem Zugriff zu schützen. Um Risiken schnell und effizient zu begegnen, brauchen Unternehmen eine umfassende Sicht auf Geschäftsprozesse, die damit verbundenen Risiken, die IT-Infrastruktur und die verwendeten Endgeräte. Eine [Security Roadmap](#) kann Ihren Schutz erhöhen.

---

## SICHERHEITSEXPERTEN

---

### Frank Heinzmann - ISSS

---



[Frank Heinzmann](#) ist seit über 25 Jahren aktiv in den Bereichen Informationssicherheit, IT Audit, IT Compliance, Governance und Risiko Management tätig. In dieser Zeit hatte er verschiedene Positionen bei Unternehmensberatungen, globalen Industrieunternehmen, Lösungsanbietern und grossen Finanzdienstleistern inne. Momentan ist er in der UBS zuständig für die Identifikation und Überwachung von Technologierisiken. Ausserdem ist Frank Heinzmann seit mehr als 10 Jahren Vorstandsmitglied der Information Security Society Switzerland, ISSS.



## Achtung, Insider!

---

Cyber-Angriffe auf die Gesundheitsbranche haben ein nie dagewesenes Ausmass erreicht und halten betroffene Organisationen auch weiter in Atem, das zeigt der «Cyber Security Intelligence Index 2016». Laut Report haben im letzten Jahr auch Cyber-Gefahren weiter zugenommen, die von Insidern ausgehen – also von Mitarbeitern oder Vertragspartnern von Unternehmen.

## Angriffe abwehren

---

Mehr Nutzer und Geräte machen IT-Sicherheit in Unternehmen komplexer. Oft erkennt man Angriffe auf das Firmennetzwerk zu spät, da die Auswertung der Datenflut schwerfällt. Durch das Zusammenspiel einer SIEM-Daten-Analyse und Netzzugangskontrolle (NAC) lässt sich die Sicherheit im Netzwerk beim lokalen Zugang oder von extern über VPN enorm erhöhen.



## Geld gegen Daten

---

CryptoLocker ist eine Ransomware, mit deren Hilfe Kriminelle die Dateien auf Ihren Computern verschlüsseln. Gegen Lösegeld bieten die Kriminellen dann an, Ihre Daten wieder zu entschlüsseln. Da Zahlen der einzige Weg ist, wieder an diese heranzukommen, ist es enorm wichtig, im Vorfeld für eine umfassende und geschützte Datensicherung zu sorgen.

## Sicherer im IoT

---

Das Internet of Things (IoT) kann praktisch sein. Es kann auch sicher sein, wenn Sie Ihrem Internet der Dinge ein eigenes Netzwerk einrichten, unkontrolliertes Plug & Play vermeiden, die Firmware aktualisieren, die Hände vom Firmennetzwerk lassen, Passwörter überlegt wählen und Geräte nur mit Internet und Cloud verbinden, wenn es wirklich nötig ist.

---

## CLOUD SECURITY

---



### Fünf Gründe für Cloud

---

Datenverfügbarkeit immer und überall, Reduktion von Kapitalkosten, Geschwindigkeit, neue Geschäftsmöglichkeiten und Skalierbarkeit ohne Kapitalbindung – das sind Gründe genug, warum der [Bedarf an Cloud-Lösungen](#) weiter steigt. Laut Experten ist es höchste Zeit, dass Unternehmen auf diesen wichtigsten Innovationstreiber für die Digitalisierung setzen.



### Angst vor der Cloud?

---

Es gibt immer noch Menschen mit [Cloud-Angst](#): Die einen sagen, die Cloud sei lückenhaft. Doch jede IT-Infrastruktur hat Lücken. Dafür sind Strategien, Konzepte und IT-Projekte da. Die anderen jammern, Bandbreiten seien ungenügend. Wenn die Abdeckung lückenhaft ist, leiden Cloud-Dienste logischerweise. Darum braucht die Wolke dringend staatliche Unterstützung.

---

## KALENDER SECURITY SCHWEIZ

---



### Wissen ist Schutz

---

Mit der Zunahme der Mobilität steigen die Risiken im Umgang mit kritischen Unternehmensdaten und -funktionen. Bei den [Resilia-Kursen](#) hören Sie mehr zu Informations-Sicherheits-Standards und lernen, wie Sie Cyber-Sicherheit umsetzen und ins Informations-Sicherheits-Management-System integrieren können.

### Kennen Sie BYOid?

---

Die wichtigsten Konsequenzen der neuen EU-Datenschutzverordnung, IT-Schwachstellen in der Cloud und Management-Systeme in der Cloud – das sind unter anderem Themen am [MEET SWISS INFOSEC!](#) von Donnerstag, 23. Juni, 13 bis 17 Uhr, im Hotel Radisson Blu am Flughafen. Namhafte Experten präsentieren Ihnen dort Erfahrungsberichte und Trends.

## Weitere Security-Termine

---

13.06.2016 - 15.06.2016	<a href="#">DuD 2016 - Datenschutz und Datensicherheit; Berlin</a>
14.06.2016	<a href="#">Information Security in Health Conference; Rotkreuz</a>
23.06.2016	<a href="#">InfoGuard Security Lounge</a>

---

[Zum Security-Kalender](#)

weitere News auf [Twitter](#)



Expertenthemen zu Cloud, Cloud-Security und Applications CRM/XRM/CEM finden Sie hier.

