Personal Invitation to 18th

swissciso summit

Cloud Security

Impact on Risks, Control and Security

28th January 2020 in Zurich

DETECON CONSULTING

pwc

SWITCH

SWISS POST

Sponsorships:

Platinum

Gold

Silver

Contents

Introduction

Dear CISO,

You are kindly invited to the 18th Swiss CISO Summit – a series of moderated round-table discussions for sharing information security practices and strategies among senior professionals.

Unfortunately we only have a limited number of places, therefore we kindly ask you to confirm your attendance as soon as possible.

B. Hämmerli

Prof. Dr. Bernhard M. Hämmerli

Cloud Security **Impact on Risks, Control and Security**	
Date	**28st January 2020**
Time	**12:00 Lunch and 13:00 Summit starts: End ca. 19:00**
Location	**Zunfthaus zur Schmiden** 1. Stock, Marktgasse 20, 8001 Zürich, Schweiz
Keynote I	**Overview of Cloud Challenges in Hybrid Cloud Environments** Andrew Hutchison, Cyber Security Specialist, T-Systems Switzerland
Keynote II	**Risk Governance as Enabler for Cloud Adoption in Sensitive Corporate Context** Rolf A. Becker, Risk Governance and Control, UBS AG
Key Benefits	• Experience industry best practices in the Swiss market • Actively participate in moderated high-level peer exchange • Understand drivers for security, gain competence and experience in discussing strategic issues • Design, develop and manage effective information security strategies for your own organisation • Receive an exclusive consolidated end of summit report detailing all the major themes discussed for re-use in your organisation
Join the Swiss CISO Summit and benefit from the peer exchange!	

2

Summary

Cloud Security – Impact on Risks, Control and Security

The perception of cloud services has changed dramatically: in the beginning, there were statements from national administrations that deeply distrusted cloud services and dis-encourage organisations to move their data and operations to cloud service providers. Today the largest banks closed a deal for their highly sensitive data with a cloud provider: the world has changed.

The gap may be explained by changes within the cloud architectures including options to use strong customer-managed encryption keys to ensure ownership and privacy for the application and data.
A purey one-to-one relation between cloud providers and organizations may be reality for some at the moment. However, a multi-cloud approach is more likely to be adopted by a majority of organizations to mitigate systemic risks, use differentiated services and optimize costs. Not a core topic, but interesting for us as individuals, we relate to multiple cloud providers (e.g. WhatsApp, Twitter, Skype, etc.) even when we are unaware of it.

We can conclude that cloud usage is today a preferred model to profit from the economy of scale effects of hardware and operating system maintenance, but even more from the highly sophisticated security management: The larger the cloud provider is, the more people work in security engineering, security operations and therefore provide a service on higher level. The numbers in the background are enormous and can be between 50 to 5.000 professional security engineers. Happily, organizations can select from a variety of service providers, such that after a contractual period, a change is feasible. But what are the exit scenarios, what needs to be prepared when already when entering the contract?

Andrew Hutchison (T-Systems) will present some of the key challenges for a hybrid cloud environment from a security perspective. Rolf Becker (UBS) will elaborate on UBS's approach considering the requirements of one of the most sensitive cloud user groups. These keynotes will introduce and stimulate the discussion with questions such as how do we negotiate with cloud providers to use of private encryption keys, how to test security concepts and how to create preparedness for switching between cloud providers.

Swiss CISO Summit – Members share from their experience

Containerization of (legacy) Applications in the Cloud for Increased Security

Security was always defined in layers. Reflecting this fact, and in addition, that the perimeter security is diluted today by cloud setups: how do companies address this challenge today? A best practice is to segment requirements and add cloud access security broker (CASB), Cloud Security Posture Management (CSPM) and Cloud Workload Protection Platform (CWPP) - for SaaS, PaaS, and IaaS respectively. Based on these segmented requirements, set up parameters for enabling to make the right choice. The Swisscard case study demonstrates that cloud security is not a replacement for perimeter security, but it is an add-on: and be aware that configuration errors might have heavy consequences. It is known in the security community that the bad actors must be kept away from your data and applications in the cloud. To achieve this- it is best to create another layer and an application (or a 'guard' if you will) who always asks to users the age old question: 'Quo Vadis'.

Amitabh Singh
CISO and CDO at Swisscard

3

Session I

Keynote

Overview of Cloud Challenges in Hybrid Cloud Environments

Most enterprises are using or considering cloud-based services for aspects of their ICT environment. The challenge is to ensure that levels of security and privacy can be preserved like an on-site situation when moving to cloud-based services. Where multiple clouds in combination with on-site services are adopted, holistic security concepts become increasingly challenging and important. The ability to retain flexibility, and potentially to swap cloud provider, is also a consideration when establishing a security architecture and environment for hybrid domains. For the Swiss market, there are special considerations and concerns around the evolution to cloud. In addition, in respect to general cloud challenges, new ideas and bridging stages for local approaches will be presented.

Roundtable Session

Understanding Cloud Security: Requirements, holistic concepts, and architectures in local context

As time progresses, we know that certain developments will progress, even when not everybody agrees on the judgment of its benefits and risks. Therefore, the discussion will focus on the security and privacy aspects of single and multihomed cloud users, its advantages of flexibility, costs, and by when the hybrid cloud should be implemented with which architecture. The discussion will address questions like “how could the dependency of cloud provider(s) be engineered, in which local architectural elements are able to provide cloud evolution, with which application is a start easy, and how to grow the number of integrated applications. The target of this discussion is an in-depth understanding of multi-homed hybrid cloud concepts with adjusted security and privacy levels.

Andrew Hutchison is Cyber Security Specialist at T-Systems Switzerland, and part of the international Telekom Security organization of Deutsche Telekom.

He advises customers regarding their security strategy, roadmap and solutions. Andrew had previously held various roles e.g. Executive Advisor Cyber Security International Programme Executive for Cyber Security, and as General Manager / Vice President of the Telecommunications Business in South Africa. Prior to joining T-Systems Andrew co-founded an IT consulting and training company, which was acquired by a South African IT group, and he has also been on the faculty of the Computer Science Department at the University of Cape Town (UCT), where he remains an Adjunct Professor. Andrew received a PhD in Computer Science (Information Security) from Zurich University while working at the IBM Zürich Research Laboratory in Rüschlikon.

4

Session II

Keynote

Risk Governance as Enabler for Cloud Adoption in Sensitive Corporate Context

Cloud adoption is an enabler for efficiency, scalability and flexibility, and survival critical in a rapidly changing business environment. Banks are one of the most regulated industries. Risk governance is an enabler for cloud adoption while at the same time responding to regulatory and client demands for transparency and control. UBS has developed a risk governance and assessment framework leveraging industry-standard cloud control requirements from the Cloud Security Alliance and the European User Group Enterprise & Cloud Data Protection in close cooperation between Business / Information Security Stakeholders with Infrastructure & Security Engineering and Technology Risk Management using Microsoft as the strategic cloud provider. This framework is applied to both internal and external cloud services.

Roundtable Session

Risk Governance and Standards: How to get the buy-in of Internal Stakeholders and align with the cloud provider

Initial for all activities in a company is a policy, in this case a cloud security policy. The first point of the policy is usually: “know your risk” and this is especially true for cloud security. But then the approaches differ, how the risk governance and standards are applied, how the CISO gets a buy-inn to the Stakeholders in the company, and how he can motivate the cloud provider to collaborate with appropriate solutions. How does “Risk Governance Cloud Security Framework” sound based on public standards, contribute to convincing the constituencies for reaching a future-oriented strategy and implementation of secure cloud services.
During the roundtable session,the goal will be an in-depth understanding of corporate cloud adaption in risk governance, security and privacy context. Thereby, internal process structure for driving cloud projects successfully forward and evidence of equal or higher standards in respect to on-site security solution are in scope and will be debated.

Rolf A. Becker is responsible for Risk Governance and Control in the UBS Group Cloud Program and for outsourcing to external cloud services.

He is co-founder and co-chair of the European User Group Enterprise & Cloud Data Protection, an opinion leader group regarding the design and use of Microsoft Information Protection in the Cloud. His previous roles were the management of the Cyber and Information Security Portfolio reporting to the UBS CISO at the global level, and the management of the Client Data Confidentiality Program Unstructured Data Protection streams. Rolf A. Becker graduated in Econometrics, Empirical Economic Research and Macroeconomics at the University of Zürich, Switzerland. His professional career encompasses over 30 years of experience in banking and founding a start-up company in flat screen technology.

5

Information

What is the Swiss CISO Summit?

The Swiss CISO Summit facilitates the exchange of current security challenges and opportunities between security executives, managers, and thought leaders in Switzerland. Each summit addresses a current hot topic. The strategic dialog and the subsequent discussions are inspired by a keynote speech from well-recognised national and international speakers. The moderated and guided discussions in groups of 8-10 members share views, experiences and strategies. An excerpt of the discussions will be written down in the result paper for the participants.
Participation is by invitation only.

How Swiss CISO Summit maintains confidentiality?

The Swiss CISO Summit is provided as a closed-door event. This exclusive CISO Executive three ticket programme is created for information security and risk executives providing them with an environment for achieving new ways of thinking and ensuring success in protecting their organisations. The summits are held strictly under the Chatham House Rules.

Why should I join the Swiss CISO Summit?

The Swiss CISO Summit has a unique concept of creating trusted circles amongst executives,managers and thought leaders. Meeting peers in an advanced business location, having time to network amongst each other and to touch current issues which are unique opportunities for sharing experiences, and for receiving advice far beyond the discussion at the table.

- Extensive networking opportunities with peers and experts on an ongoing basis
- Meet with other leading executives to share successes, failures, obstacles, and challenges
- Learn about current strategies on managing security threats and to prepare for the future
- Make new connections and equip yourself with information on recent projects and achievements

What makes the difference?

The Swiss CISO Summit has many and diverse benefits for the invited experts. The participants are the focal point of the summit and the meeting is not intended for providers to present solutions or products. Sales are strictly prohibited to the good of an open and free CISO information exchange.

What is the history behind the Swiss CISO Summit?

The Swiss CISO Summit has been run successfully since 2001 under the name «Risk and Security Exchange» and from 2004 - 2009 when it was known as „Swiss Security Exchange“. Then with the financial turmoil the summit came to a halt. From 2009 onwards, the same successful format was adopted in Norway where it ran under the name „Sikkerhetstoppmøte“. All this experience gained by Prof. Dr. Hämmerli is put into the organisation of the Swiss CISO Summit.

5

Information

Who prepares and facilitates the Swiss CISO summit?

An organising committee under the lead of Prof. Dr. Bernhard M. Hämmerli is responsible for the invitation, preparation and guidance of the discussions. He is an internationally well-recognised expert with 25 years of experience in information security in governments, industry and academia. He led the Cyber Security activities of the Swiss Academy of Engineering Sciences SATW from 2012 – 2017.

Prof. Dr. Hämmerli is a founding member of the Information Security Society Switzerland and he built up the first Information Security master programme in Lucerne in 1996, respectively 1999, and since 2017 he is head of the new BSc Information & Cyber Security at Hochschule Luzern/Informatik. Additionally, he teaches at the Norwegian University of Science and Technology Norway www.ntnu.no, in the technology and management track of the Information Security master programme.

Prof. Dr. Hämmerli is supported by Katarzyna Kuhn for administrative purposes.

Agenda (generalised)

12:00 Start with a small lunch
13:15 Welcome and introduction
13:20 Keynote from experts or members
14.30 Roundtable session I
15:25 Exchange between the groups and wrap-up of roundtable I
15:40 Break
16:00 Roundtable session II
16:55 Exchange between the groups and wrap-up of the roundtable II
17:10 Summary note
17:30 Cocktail and aperitif

The meeting is held three times per year.

6

Sponsorships

Platinum Sponsor	**Detecon**
DETECON CONSULTING	Detecon Consulting is one of the world's leading management consulting companies for integrated management and technology consultancy. Detecon (Schweiz) AG is located in Zurich and bundles Financial Management as well as ICT Management competences among its roughly 150 employees. The main focus lies on the requirements of CFOs and CIOs in nearly all industry sectors.Globally, more than 6000 projects have been implemented successfully. The international spirit and the openness are reflected not only in the number and origin of our clients from over 160 countries but also in our employees that are recruited from 30 different nations.
Gold Sponsor	**PricewaterhouseCoopers**
pwc	At PwC, our purpose is to build trust in society and solve important problems. PwC looks at cyber security as one of the biggest challenges to solve in today's times and provides a full stack of cyber security consulting services. PwC's Cyber security practice comprises deep information security, forensic technology, business and technology resilience, Cybercrime response, technology risk and controls, project and program management and operations specialists to help clients address Cyber risks through the whole lifecycle from strategy to execution and operations.
Silver Sponsor	**SWITCH Foundation**
SWITCH	The foundation "SWITCH" was founded in 1987 under private law by the Swiss Confederation and the university cantons and is an integral part of the Swiss-academic community. Based on our core competencies network, security and identity management, SWITCH offers collaboratively developed ICT solutions that empower users in and beyond the academic world to achieve leading edge results in a globally competitive environment. SWITCH's Computer Emergency Response Team (SWITCH-CERT) is one of the most experienced CERT and besides the government CERT MELANI, one of two National CERTs in Switzerland.
Silver Sponsor	**Armed Forces Command Support Organisation (AFCSO) Führungsunterstützungsbasis (FUB)**
FUB	With its services in ICT and electronic operations, the Armed Forces Command Support Organisation (AFCSO) ensures that the armed forces can accomplish their missions. It guarantees the command and control of the armed forces under all conditions.
Silver Sponsor	**SWISS POST**
SWISS POST	Swiss Post is part of the critical infrastructure of Switzerland. On top of its logistics and transport services, Swiss Post offers a variety of digitalized services in other industries ao. electronic voting, eHealth and secure eMail. The ICT department holds certificates on ISO 27001, 22031 and 20000. Information Security is an integral part of all activities of Swiss Post Group. As a first mover in the Paris Call for Security and Trust in Cyberspace, Swiss Post Group fosters expertise sharing on security in trusted environments both nationally and internationally.

Registration

Join Swiss CISO Summit

Participation is by invitation only. We accept proposals for new participants. The number of participants is limited to 40 per summit in order to maintain an atmosphere of trustful information sharing.

Single summit CHF 450.– per participant
Three summits CHF 1'000.– per participant (25 % discount for booking three consecutive summits – not three participants at the 18th summit)

Cancellation Policy

Cancellations of registrations are free of charge only if received no later than seven days before the summit. Cancellations received beyond this point will incur 100 % of the admission fee. In any case a delegate may be sent at no additional cost. More information is found at www.ciso-summit.ch. Content responsibility for the summits lies with Prof. Dr. Bernhard M. Hämmerli.

Register by just replying to the invitation email with all your details or by following these steps:
Step 1: Fill out & save the form
Step 2: Select Send button > email opens (info@ciso-summit.ch)
Step 3: Attach the PDF file

Registration

PRINT RESET SEND

Register by just replying to the invitation email with all your details – or by filling out this form and mailing it to info@ciso-summit.ch.

☐ **Three consecutive summits for CHF 1'000.–**
3 events, Summit 18 (28.01.2020), 19 (12.05.2020) and 20 (17.10.2020)

☐ **18th Swiss CISO Summit, January 28th, 2020 for CHF 450.– (single event)**

First Name _____ **Surname** _____

Organisation _____

Street / No. _____ **ZIP / City** _____

Phone _____ **Email** _____

Signature _____ *Date* _____

swissciso summit

More information is found at www.ciso-summit.ch

Sponsorships:

Platinum

Gold

Silver