Personal Invitation to 13th

swissciso summit

IoT and Industrial Control Systems (ICS) – Concepts, Risks, and the new Role for the CISO

29th May 2018 in Zurich

DETECON CONSULTING

pwc

FUB | SWITCH

Sponsorships:

Platinum

Gold

Silver

Contents

Introduction

Dear CISO,

I would like to personally invite you to the 13th Swiss CISO Summit – a series of moderated roundtable discussions to network and share information on security practices and strategies amongst senior professionals.

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

Prof. Dr. Bernhard M. Hämmerli

IoT & Industrial Control Systems (ICS) – Concepts, Risks, & the new Role for CISO	
Date	**29th May 2018**
Time	**12:00 pm**
Location	**Radission Blu, Airport Zurich** (5 walking minutes from Zurich Airport train station, parking available)
Keynotes	**IoT concepts, security and its integration into enterprise security architecture: Incidents, mitigation strategies, and corporate roles with respect to security.**
Speakers	**Angela Nicoara**, Head of IoT Labs at Hochschule Luzern / Informatik **Gregor Nyffeler,** Head of IT Services within the Zurich Municipal Electric Utility (ewz)
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!

Summary

IoT and Industrial Control Systems (ICS) – Concepts, Risks, and the new Role for the CISO

Internet of Things (IoT) services, Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) are connected today to internet via the corporate network. In many corporations these systems are in separate network security zones, with strong firewalls in-between. The security risks of these technologies come from many sides, internal devices as well as mass installation from outside such as DDoS attacks from COTS cameras world-wide directed on a few servers. For both security risks CISO must elaborate security plans. With two leading speakers, one from research and innovation, one from an early adopter of the upcoming technologies the discussion at the round table will be introduced and stimulated.

IoT services, Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA), Industry 4.0 and Digital Transformation are pending issues in any enterprise, and future business success will depend on timely and proper application and integration of these new concepts. In this context the CISO's organisation must be included in such projects and provide solutions for security and resilience in the three phases „protect, detect and response".

As usual, the goal of Summit 13 is to learn from the speakers, from each other and from the background material which will be distributed before the meeting for exploring today's baseline and designing effective and efficient security solutions in these new fields.

Session I

Keynote

IoT concepts, security and its integration into enterprise security architecture: Incidents, mitigation strategies, and corporate roles in respect to security.

IoT is the largest computing revolution and will grow up to 20.4 billion devices by 2020. Against this background, in this talk we present the challenges, threads and risks in resource-constrained IoT settings, the importance of security in IoT, and give three real-world use cases from different industries and major security flaws and past incidents. The question "why is it hard to apply correctly measures against the CIA triad" is explored, as well as issues with the authentication mechanism. We conclude with the giving options on responsibilities of IoT security: What is the role of the supplier, the customer architect, the customer operator, the CISO? In preparation for the discussion, positions are given to these questions, as well as it is pointed out, that IoT will penetrate all industries, also typical information processing industries like administration, insurances and banks.

Roundtable Session

Identifying relevance of IoT in the context of Digital transformation and responsibilities

IoT with its enormous growth and perspectives in digital transformation, Industry 4.0 and exploration of future business models will be reflected in the context of opportunities for the enterprises of present CISO at the tables. After identifying top IoT business development opportunities the discussion will be on the analysis system architecture and potential risk of the new technologies. The role of the CISO in this new context with collaborating units such as operations, system architecture and business development will conclude the first round.

Angela Nicoara, Head of elaborating corporate roles and responsible for IoT Systems & Software Research at Hochschule Luzern / Informatik (HSLU-I), has been building breakthrough technologies in IoT, mobile, and distributed systems from inception to widespread adoption (at Intel, Deutsche Telekom, Google, ETH Zurich, Caatoosee, WebQuote, HSLU-I).

She received many awards and honors as e.g. Intel Division Recognition Award, Women in IT Awards USA - Finalist - "Innovator of the Year" (top 10 women innovators in USA), Best Paper Awards from IEEE RTAS and ACM WWW DT Innovation Award. Her very rich work (publication, conferences, industry) has been quoted by press and media. Angela made her PhD at ETHZ.

Session II

Keynote

Securing IoT, ICS and SCADA: Analysis, measures, detection and integration into corporate processes?

The Zurich Municipal Electric Utility (ewz) is an enterprise which has had Industrial Control Systems (ICS) for a long time and is also an early-adopter for Internet of Things (IoT) services. Understanding the landscape leads to security challenges with ICS / Supervisory Control and Data Acquisition (SCADA). The list of topics to be addressed is large, and starts with understanding risks and architecture, applying counter-measures, performing detection and reaction. The proof of well-functioning security orchestration is the everyday experience with its integration into the corporate processes. The presentation will cover several hands-on cases before and after addressing the issue properly, and will demonstrate the potential of securing ICS/ SCADA. In addition, monitoring tools, their user interface and how conclusions can be drawn from the tools, will be shared with the audience. The overall understanding of security and how it is achieved in a distributed organization like ewz, will conclude the speech.

Roundtable Session

Securing IoT, ICS and SCADA: analysis, detection and response in the corporate context.

IoT, ICS and SCADA security is of top priority, after connecting such devices to the corporate network. The traditional air-gaped ICS / SCADA network has disappeared, and new concepts consider the daily back and forward of data and updates also as extension of the corporate network. Therefore, its security must be re-thought and enhanced with proper detection and responses. In this context the discussion will be on air-gap, security concepts, detection and response, as well as the design and anchoring of these issues in corporate processes and structures for creating an effective and efficient overall security solution.

Gregor Nyffeler is the Head of IT Services within the Zurich Municipal Electric Utility (ewz), Switzerland. He holds a Master of Science from University of Bern in Biology. He has been in the IT industry for the last 22 years and has held management positions in Finance, Retail and Academia.

Currently, he is focusing on the digital transformation with its new area of business/commerce and the impact of future ICT-Services on IT Security.

Registration

Join Swiss CISO Summit

Participation is by invitation only. We accept proposals for new participants. The number of participants is limited to max. 40 per summit for maintaining 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)

Cancellation Policy
Cancellations of registration are free of charge but 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, however, 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

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.
Email address: info@ciso-summit.ch

☐ **Three consecutive summits for CHF 1'000**
3 events, Summit 13 (29. 5. 2018), 14 (30. 10. 2018) and 15 (30. 01. 2019)

☐ **13th Swiss CISO Summit, May 29, 2018 for CHF 450.–** (single event)

First Name _____ **Surname** _____

Organisation _____

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

Phone _____ **Email** _____

Signature _____ *Date* _____

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. The summits are held strictly under the Chatham House Rules, which is the ruleset to treat the shared information with full discretion.

- 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 the current strategies on managing security threats today and to prepare for the future
- Make new connections and equip yourself with insider 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 today’s Swiss CISO Summit.

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 today is the Head of the new BSc Information & Cyber Security at Hochschule Luzern / Informatik. Additionally, he also teaches at the Norwegian University of Science and Technology 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
13.30 Keynote from experts or members
14.20 Roundtable session I
15.20 Exchange between the groups and wrap-up of roundtable I
15.40 Break
16.00 Roundtable session II
16.50 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.

Sponsorships

Platinum Sponsor	**Detecon**

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**

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**

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)**

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.