Personal Invitation to 16th

swissciso summit

Third Party Security and Patching:
How to face this major vulnerability?

21st May 2019 in Zurich

DETECON CONSULTING

pwc

SWITCH

FUB

SWISS POST

Sponsorships:

Platinum

Gold

Silver

Contents

Introduction

Dear CISO,

You are kindly invited to the 16th Swiss CISO Summit – a series of moderated round-table discussions for sharing information security practices and strategies among senior professionals.

Please be informed that we have only a limited number of places. Therefore we kindly ask you to confirm your attendance as soon as possible.

Prof. Dr. Bernhard M. Hämmerli

Third Party Security and Patching: How to face this major vulnerability?	
Date	**21st May 2019**
Time	**12:00 Lunch and 13:00 Summit**
Location	**Radisson Blu Hotel** Airport Zurich, Rondellstrasse, 8058 Zurich, Switzerland
Keynote I	**Vendor Risk Management** Guy Kelleter, Risk Manager 3rd Party, AXA Winterthur
Keynote II	**Third Party Information Security for Swiss Universities** Martin Leuthold, Head of Network & Security, Switch
Key Benefits	• Experience industry best practices in the Swiss market • Participate actively 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 organization

Join the Swiss CISO Summit and benefit from the peer exchange!

2

Summary

Third Party Security and Patching: How to face this major vulnerability?

In analyzing root causes of incidents, third party security and patching is strongly represented as a solution to attacks around 80% of the time. It is, thus, an utmost and urgent issue that needs addressd.

From the perspective of attackers, it is essential to run the attack-business well, which is why they invest 10-20% of their time investigating the weakest point in the targets' defense concepts. Well protected multi-billion-dollar global companies are hard targets to hit, but their suppliers, their contractors, their clients and partners are often protected on a SME level only.

Against this background, the weakest links are often represented by a third party, which is an ideal situation for hackers to get an easy hook in to the well protected castle.

There are many statistical reports on patching., With an observed share of 50% of patched systems functioning 10 days after a patch has been implemented, it is clear that the patching sequence is in many cases far less effective than what it should be. However, the other 50% of systems are vulnerable with known weaknesses for which attack suits can be downloaded from the internet or the darknet. For any hacker, these are easy targets that can be conquered at very low cost.

The theory behind the topic is really very easy to understand, however, counter measures need many careful steps. There are two enlightening presentations on this topic in this summit. The first one deals with third party and patching issues in procurement and creates a binding framework for security issues in partnerships. The second one is based on real-time measurements in which the partners are controlled with software and information will be presented on the real important issues of how the observed weaknesses can be presented and eliminated.

As usual, the goal of Summit 16 is to learn from the speakers, from each other and from the material distributed before the meeting in order to explore today's most compelling trends in addressing the information and cyber security challenges with the best set of controls.

3

Session I

Keynote

Vendor Risk Management

Either by crafting APTs or by seeking for the weakest partner in a cross-linked network, attackers search for many opportunities to blend in company's infrastructure. Just by listening to the ongoing traffic gather due information to finally exfiltrate the desired data they are looking for. Most recently some most likely politically motivated hacker groups started to create chaos and damage only: the collected data were no more used for getting money.

Even a company like J P Morgan, investing 200 Mio US$ for security per year, where hit anyway by an APT. Also, Swisscom encountered a data leakage, because one of their suppliers was not well secured. Threats are facing an enterprise from everywhere and reaction to incidents must be immediate. In contrast, attackers have plenty time to analyze their targets, develop their approach, and finally for creating their success.This means that we cannot be absolutely save but we can reduce as the attack vectors and make sure, to detect intrusions as soon as possible.

Beside monitoring and observing our own infrastructure, we select suppliers wisely and reassure, their risk footprint does not worsen during the coming years. For this purpose, AXA defined processes for evaluating suppliers and for generating contracts: the overall all goal is to assure they take responsibility for security. Through these processes we guarantee a sound Vendor Risk Management.

Guy Kelleter will present the approach, taken by AXA to manage its vendor risks. He'll show the framework that was build and the organization that is in place, to deal with the need to manage the outsourcing initiatives and involved parties.

Roundtable Session

Contract based Vendor Risk Management: Needs, Borders and Limitation

What are various options by today in industry for vendor risk management? Do smaller enterprises have a chance to control its vendors? Are services needed to control vendors, or must asymmetric contracts just be accepted? Which methods works to get a buy-into to the vendors, such that clients get their support for implemented products. Are there any liabilities, from which vendors cannot withdraw? Would associations (e.g. CISO or industry sectors help, to have more power on the vendors?).

Guy Kelleter graduated in Electrical Engineering as a technician in Belgium and worked for the next seven years as an industrial electrician, building machine control systems and installing machines in the industry. Upon his move to Switzerland, he followed education in different programming languages and worked as a programmer on mainframes. He got the mandate to instruct junior programmers and was promoted to the chief programmer in the international department. A couple years later, he was proposed for the position of a personnel manager, which he kept for more than 5 years. He went back into IT, especially in Web application security, where he wrote policies and guidelines. Form then on-going he has worked in security, and manages a team of 12 people in UK and CH. In January 2009, he obtained the certification as a CISSP.

His has about 30 years of management experience in IT and information security in an international company, including the CISO role in a technical area. In July 2018, Guy Kelleter took over a new established role as an IT Risk & Security Manager, with the main purpose of managing the vendor risks and vendor selection.

4

Session II

Keynote

Third Party Information Security for Swiss Universities

Recent cyber security incidents indicate a fast-developing trend of indirect attacks on company through their vendors. Reason for that are improved proactive security measures and raising defense capabilities of many (larger) organizations and companies. Attackers, seeking to minimize effort to reach their attack targets, are increasingly targeting (smaller) third party service provider with lower defenses.

From there, they are moving laterally into their target organizations by misusing access credentials of these third-party service providers. Such attacks are often difficult to detect as the might show similar behavior patterns as normal cooperation.One measure to (partly) mitigate and minimize these risks is a systematic third-party information security monitoring. Scope is on watching trends and comparing targeted 3rd parties within their vertical.

To be effective, an interdisciplinary approach is needed, combining information security and ICT-security knowledge and experience with legal and procurement capabilities because vendor management and a good contract and SLA basis are key to success. The presenter is currently discussing a joint approach to Third Party Information Security Management within the CISO community of SWITCH (CISOs of Swiss universities and research organizations) and will provide some insight on the targeted setup and value propositions.

Roundtable Session

Real-Time Third-Party Risk Management: An Urgent Need or an Overkill?

Which aspects are covered by contract base third party risk management? Which functionality are in addition available with real-time tool based third party risk management? What are the differences of third-party real-time monitoring tools? Which options are available to request third-party to react on observed security vulnerabilities? Which indicators show that executive management must support the CISO in a case? Which role play national authorities in theatre of third-party risk management? In case of using cloud-based data center services, what are the differences of the main models SaaS, PaaS and IaaS?

Martin Leuthold graduated in Electrical Engineering as MSc ETHZ and completed later post-graduate studies in information technologies and graduated as Dipl. NDS in Informationstechnik ETHZ. Since 2008, he is certified by ISACA as CISM. He is member of the SATW cybersecurity platform and advisory board, member of the cybersecurity commission of ICTswitzerland and member of the Telecom Service Provider Department, ICT division of the Federal Office for National Economic Supply (FONES).

In February 2016, Martin Leuthold joined SWITCH as member of the executive board in the role of Head of Security and CISO. Since January 2017, his responsibility has been extended to Head of Network and Security. He is therefore responsible for engineering and operations of the National Research and Education Network (NREN) of Switzerland and for SWITCH-CERT, one of the leading CERTs in Switzerland, listed besides MELANI as a National CERT by Carnegie-Mellon University. As CISO, he is responsible for SWITCH ISMS that is ISO 27001 certified in the scope of the Domain Registry.

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 (please contact Bernhard Hämmerli for participation). This exclusive CISO Executive 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 which is the ruleset to treat the shared information with full discretion, and for providing secrecy against non-group persons.

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
12:30 Networking Session
13:00 Welcome and introduction
13.30 Keynote from experts or members
14:00 Roundtable session I
15:00 Exchange between the groups and wrap-up of roundtable I
15:10 Break
15:40 Keynote from experts or members
16:10 Roundtable session II
17:05 Exchange between the groups and wrap-up of the roundtable II
17:15 Summary note
17:30 Cocktail and aperitif
19:00 End

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 16th 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 16 (21.05.2019), 17 (15.10.2019) and 18 (28.01.2020)

☐ **16th Swiss CISO Summit, May 21st, 2019 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

DETECON CONSULTING

pwc

Gold

SWITCH

FUB

SWISS POST

Silver