Personal Invitation to 20th

swissciso summit

Ransomware & Malware:

Prevention, Early Detection & Response

Which Strategies are successful?

4th November 2020 in Bern

DETECON CONSULTING

pwc

SWITCH

SWISS POST

Sponsorships:

Platinum

Gold

Silver

Detecon (Schweiz) AG
Löwenstrasse 1
8001 Zürich
Schweiz
www.detecon.ch

Contents

Introduction

Dear CISO,

You are kindly invited to the 20th 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

Ransomware & Malware: Prevention, Early Detection and Response: Which Strategies are successful?

Date	**4th November 2020**
Time	**12:00 Lunch and 13:00 Summit, end approx. 19:00**
Location	**Sorell Hotel Ador** Laupenstrasse 15, 3001 Bern
Keynote I	**Ransomware – Necessity and chance for a matured cyber security strategy** Frank Herberg, Head of SWITCH-CERT (Commercial Sectors)
Keynote II	**Fighting criminals – Experiences from a true war story** Johannes Dohren, Director Cybersecurity at PwC
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!

Summary

After a longer period of E-banking fraud, the resistance of the merging better protected E-banking against the hacker's penetration attempt was increasing so much, that the business model did not work out for the hackers anymore. The hackers needed to find a new source for their income.

The new source is primarily ransomware, which made them develop trojan horses, install them on the victim's system, and encrypt the data of the system. The victim cannot work anymore and does not see his data. At this points the hacker start negotiating, how much money they want, for releasing the crypto keys, such that the victim can reuse his data.

Customers having a real offline backup, just install their data again, and work further. But there are quite a few corporations having mirrored server system, which protects very well against hard drive failure, but not at all against crypto locker software.

A crypto locker ransomware as well as other ransomware (e.g. payment for not publishing of embarrassing or confidential data) needs time to be placed in an evaluated system. This system selects hackers very carefully. And several steps are needed until the final key will be pressed when all data encrypt. During this period, Computer Emergency Response Teams (CERT) and Security Operation Center (SOC) may find indicator of compromise and can potentially mitigate the upcoming catastrophe.

Our debate will examine strategies which were successful in specific cases and share strategies which not succeeded before the system was under hacker's control. And we will look at these strategies before the incident happened and at the response: How to negotiate with the hackers, how to start fighting, what means fighting for the victim, and how likely is success? How does the requested amount change when the fight continues for longer time? Which type of support we need in such situation, and how we can get this support? And is it wise to look for partners before the incident?

The first presentation from Frank Herberg (Switch) prepares the ground for broad discussion, how detection of indicators of compromise work, and how to respond to these. In addition, some response options are debated. The second presentation from Johannes Dohren (PwC) presents a true war story and demonstrates lively "what fighting against hacker" really means.

With this setup we expect to serve the community with an inspiring exchange for being better prepared and have more options to react on hackers attempt to harm us.

3 Session I

Keynote

Ransomware – Necessity and chance for a matured cyber security strategy

Ransomware attacks developed in recent times from widely dispersed attacks with repetitive attack vectors to targeted attacks with individual tailored patterns. For attackers it's apparently a worthwhile investment to explore their victim's infrastructure, crown jewels and financial solvency as a preparation to the actual ransomware attack. On the detection and response side of the game this means that we can't rely on baseline security measures, offline-backup and a static cyber security roadmap anymore. It's rather important to learn continuously from the likewise agile development of the attacks and use this gained knowledge to review and re-align defense measures: This means realigning priorities and leading the justification debate. Given recommendations will support you in your analysis phase with a systematic approach, applicable to your own environment. The aim is identifying potential quick-win improvements and to supporting you in reprioritization of planned security measures.

Roundtable Session

Malware and Ransomware: from recognizing indicators of compromise to incident and to reaction options: when is success likely?

The corporations are each year more and more badly attacked, with increasing financial losses, despite upstaffing security functions: a real nightmare for managers who want acting in a time shot, and having the challenge fixed. Recognizing indicators of compromise, verifying false positive and perusing consistently the others with an appropriate response is the target. Which reporting and communication channels must be followed to include management successfully? Which options we have for getting better in the ever-lasting race between hackers and potential victims? By when we need help from others, and how to prepare the contracts? When we should open-up to authorities? What changes with mandatory incident notification to authorities? Which recommendation you can share amongst each other?

The target of this discussion is an in-depth understanding of the malware and ransomware scenario and with a deep understanding of peer's preparedness.

Frank Herberg, Head of SWITCH-CERT joined SWITCH in 2012. He leads CERT (Commercial Sectors), one of the two national Computer Emergency Response Teams in Switzerland. With a team of 20 security engineers SWITCH-CERT helps its customers from the sectors Research & Education, Banks, Energy and Industry & Logistics to prevent and respond to cyber security incidents. Prior to this role, he worked as a Consultant and Consulting Manager several technology projects for banks, large industrial companies and technology startups.

Session II

Keynote

Fighting criminals – Experiences from a true war story

On a Friday morning like any other, the senior management of one of our clients called us explaining that they had been attacked. Our specialists lost no time and responded remotely as well as on-site with the client. What followed were days of defending the network and analyzing the attack to safeguard the infrastructure and find out what really happened. What felt like a Hollywood movie to the client left them with difficult decisions and the realization that no plan survives contact with the enemy – especially when the enemy is ready to fight.

Looking at this attack from two angles, from the attacker's and the defender's perspective. Analyzing along the cyber kill chain what happened during this attack to one of our clients – from the moment of detection, looking into the immediate necessary actions and learnings of the initial response and the longer-term intense fight against the criminal actor. The story of the good, the bad and the ugly of an incident response case during COVID-19-times.

Roundtable Session

Response: Strategies, acting options, evaluation, and recommendations

Response is case specific, and each case is different. However, in case of ransomware, many reactions have in common a fight of several weeks against the attacker, which is an extremely hard time for internal response teams and external supporters as well as for all other employees, which have to adapt to different work processes. Therefore, the debate on strategy selection, selection of acting options is the key for later success. From the presented case we learn, what worked out and what have been failing attempts. We will enlarge in the discussion these patterns, and add side effects, which might be not known for the audience.

The final target of the debate is to present a potpourri of options, which has proven as good and which has been failing.

Johannes Dohren, Director Cybersecurity at PwC is leading the Cyber Resilience and Incident Response practice at PwC Switzerland. Over the last decade he has gained comprehensive insights into offensive cyber operations and helped companies develop security strategies to protect their most valuable assets.

Johannes has extensive experience investigating cyberattacks and cooperation with national and international law enforcement agencies. He understands security as business enabler and the top management of various organizations has placed their trust in him when it comes to cyber security. Among other things, he was responsible for the cyber security of a financial services company and the attack detection and defence of a risk-exposed online portal. Based on his educational background in computer science and previous roles Johannes has in-depth technical knowledge as well as management experience. In 2018, he founded CYBER:HUB, an association to promote awareness in the technology sector with a focus on cyber security. In addition, he is a lecturer in "Digital Risk Management" and "Mobile Security" at the University of Applied Sciences in Business Administration Zurich.

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.

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
12:45	Networking Session
13:15	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 20th 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 20 (4.11.2020), Summit 21 (26.01.2021) and Summit 22 (01.06.2021)

□ **20th Swiss CISO Summit, November 4th, 2020 for CHF 450.- (single event)**

First Name ______________________ **Surname** ______________________

Organisation ____

Street / No. ______________________ **ZIP / City** ______________________

Phone ______________________ **Email** ______________________

Signature ______________________ *Date* ______________________ swisscisosummit

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

DETECON
CONSULTING

pwc

SWITCH

SWISS POST

Sponsorships:

Platinum	Gold	Silver
DETECON CONSULTING	pwc	SWITCH SWISS POST