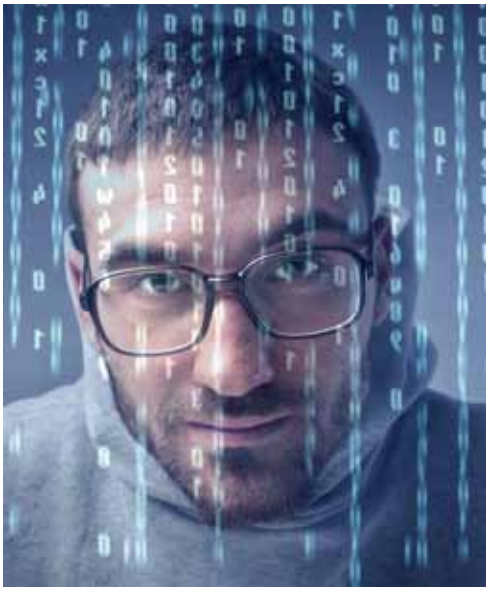
CYBER ATTACKS AND DEFENSE

SWISS CYBER STORM

WWW.SWISSCYBERSTORM.COM

Meet the Future Cyber Talents!



Swiss Cyber Storm 4 - Security Conference

June 13th, 2013 @ KKL Lucerne

Schweizer Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Informatiksteuerungsorgan Bund ISB
Nachrichtendienst des Bundes NDB

Melde- und Analysestelle Informationssicherung MELANI

spik
Swiss Police ICT

Editorial

Bernhard Tellenbach

President Swiss Cyber Storm Association

How can we protect ourselves from current and future cyber threats? How can we take appropriate actions to combat these attacks?

We need professionals who are not intimidated by the highly dynamic and complicated topic. We need professionals who will network, who are willing to further their education and do not shy away to include political discussions into their specialty area. In other words: We need YOU!

With Swiss Cyber Storm 4, the Swiss Cyber Storm Association wants to contribute in providing a suitable platform where you can obtain and exchange information and network with regard to current cyber risks and topics. In an effort to create a more interactive informational environment, we have scheduled enough time for discussions and questions after each speech. Please take this opportunity to ask questions and introduce your experiences and suggestions in the discussion forum.

If we would like to engage the necessary professionals in the future, IT security must compete against many others for the greatest talents; in part, with more "visible" professional areas and careers for young people. The goal of the Swiss Cyber Storm Association is to make a contribution by addressing the IT security topic with students and motivating the students to contemplate this topic. Therefore, Swiss Cyber Storm has launched the Security Alpen Cup in cooperation with Austria. Following an online-qualification phase the best up-and-coming Swiss talents will be selected during half-time at the Swiss Cyber Storm 4. These individuals will then compete against the best talents from Austria during the finals in November. The competition will not be limited to Switzerland and Austria in the future. The prospects of other countries joining the competition in time for Swiss Cyber Storm 5 next year are great.

Swiss Cyber Storm 4 already provides adequate opportunities to network with tomorrow's IT talents today. Accommodate the curiosity and inquires of young talents!

Cyber Storm Agenda

Time	Track 1	Track 2	Track 3
0800 - 0830	**Registration**		
0830 - 0930	Costin G. Raiu (Director of Kaspersky Lab's Global Research & Analysis Team) **Advanced Malware Cyberespionage: From Flame and RedOctober to Miniduke**		
0930 - 1015	Michael Anti (Chinese Blogger) **Cyber Security and Censorship: The Unconventional War**		Cyber Challenge - Final -
1015 - 1040	**Coffee Break**		
1040 - 1105	Candid Wüest (Symantec) **Targeted attacks: How sophisticated are they really?**		
1105 - 1130	Dr. Thomas Maillart (UC Berkeley) **On the Importance of Human Timing for Quantitative Cyber Risks Management**		
1130 - 1215	John Matherly (Shodan) **Internet Cartography: Using Shodan to Explore Uncharted Territory**		
1215 - 1315	**Lunch**		
1315 - 1400	Dr. Timo Steffens (CERT DE) **APT campaigns**	Dr. Stefanie Frey, (MELANI) **Implementing the National Strategy for Protection of Switzerland against Cyber Risks**	Cyber Challenge - Final -
1400 - 1445	Yaron Blachman (PwC) **Cyber Threat Intelligence – Buzzword or Real Thing?**	Dr. Michael Pilgermann (BMI) **Implementing a Cybersecurity Strategy in CIIP**	
1445 - 1515	**Coffee Break**		
1515 - 1600	Oliver Münchow (InfoGuard) Manuel Krucker (InfoGuard) **APT live – An in-depth example of an professional inside-out attack**	Dr. Stefan Lüders (CERN) **Why SCADA security is NOT like Computer Centre security**	Finalists must present their work to the jury - Appraisal -
1600 - 1645		Mark Tibbs (SOCA) **The Industrialisation of Cybercrime**	
1645 - 1745	Swiss Cyber Storm Podium & Swiss Cyber Talent Award Ceremony		
after 1745	**Apéro Riche**		

Swiss Cyber Storm Patronage

MELANI

Schweizer Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Informatiksteuerungsorgan Bund ISB
Nachrichtendienst des Bundes NDB

Melde- und Analysestelle Informationssicherung MELANI

MELANI, the Reporting and Analysis Centre for Information Assurance is supporting Swiss Cyber Storm because of its cyber talent initiative and research presentations in the field of critical infrastructures, incident handling and law enforcment.

Swiss Police ICT

Swiss Police ICT is an association of representants from different police corps and companies active in the IT business.

A political advisory board consisting of representants from the five parties of the Federal Council, a senior civil servant and a police commander. The board is consulted in political matters and it helps to establish and maintain links to politicians.

Moderator

Mark Saxer - lic. phil. I

Mark Saxer is general manager of Swiss Police ICT and one of the founders of SPIK, the Swiss Police Informatics Congress. Since many years, the political scientist deals with the question of public safety in the digital age.

He is a partner and senior consultant at Furrer.Hugi & Partner, a public affairs agency, where he mainly works on projects in the domain of IT and security. Furthermore, he works as a coach for communication, moderation and presentation techniques.

About Swiss Cyber Storm Association

The Swiss Cyber Storm Association was founded last November 15th, 2012 as a Swiss non-profit organisation. It is our goal and mission to setup and run a high profile Cyber Security conference in Switzerland and bring together young cyber talents with the representants of European governments, police, law enforcment, decision makers and IT security professionals. Together with Cyber Security Austria we are developing the „DACH Cyber Security Championship“ and are open for other European countries to participate.

Keynote - Costin G. Raiu, Kaspersky Lab

Costin G. Raiu - Director, Global Research and Analysis Team (GReAT) Kaspersky Lab

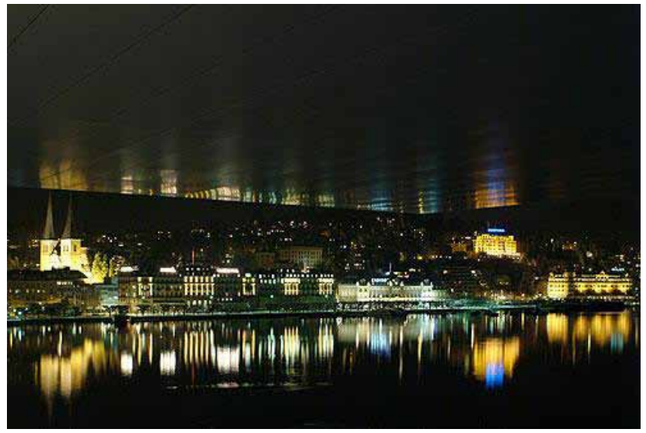
Keynote: Advanced malware cyberespionage: From Flame and RedOctober to Miniduke

Costin specializes in analyzing advanced persistent threats and high-level malware attacks. He is leading the Global Research and Analysis Team at Kaspersky that researched the inner workings of Stuxnet, Duqu, Flame, Gauss and more recently, Red October. Costin's work includes analyzing malicious websites, exploits and online banking malware. Costin has over 17 years of experience in anti-virus technologies and security research. He is a member of the Virus Bulletin Technical Advisory Board, a member of the Computer AntiVirus Researchers' Organization (CARO) and a reporter for the Wildlist Organization International. Prior to joining Kaspersky Lab, Costin worked for GeCad as Chief Researcher and as a Data Security Expert with the RAV antivirus developers group. Costin joined Kaspersky Lab in 2000. Prior to becoming Director of the Global Research & Analysis Team in 2010, Costin held the position of Chief Security Expert, overseeing research efforts in the EEMEA region. Some of his hobbies include chess, high precision arithmetic, cryptography, chemistry, photography and the Science Fiction literature.

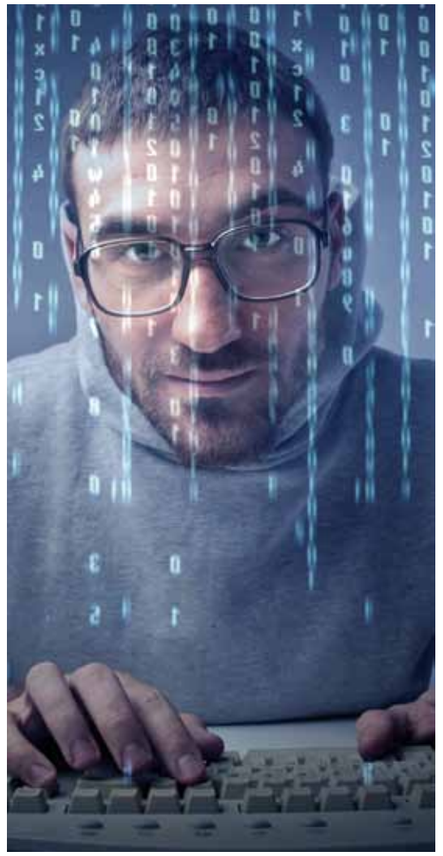
Apéro Riche - KKL Lucerne Terrace

KKL luzern

Starting from 17:45, Swiss Cyber Storm offers an Apéro Riche on the KKL Lucerne Terrace. The Lucerne Terrace is an exceptional location with fantastic perspectives. Enjoy a glass of wine, a beer and small intermezzi when you discuss with our speakers and conference attendees. And don't forget to enjoy the view on the breathtaking skyline of Lucerne!



Meet The Future Cyber Talents



Austria and Switzerland are competing in the Alpen Security Challenge 2013. Finding the Future Cyber Security Talents is cruicial in both countries' cyber defense programs. But how do we find them? How do we get in touch with these talents? The idea of an Internet security challenge is born.

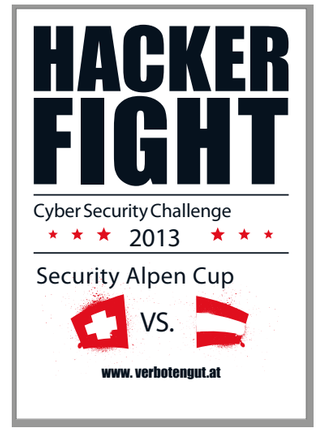
Back in February 2013, Swiss students were being invited to proof their security skills in Hacking-Labs remote security lab. In several online puzzles, the contestants have proofen their in-depth knowledge in the field of cyber security. They earned points for successfully solving the so-called online security challenges. We have invited the leading 10 players to compete in this years Swiss Cyber Storm Challenge final! In parallel to the lecturing talks, the contestants will be challenged again with more complex security puzzles and fight for the Swiss Cyber Storm champion. They have worked as individual during the online qualification, but now the rules have changed. They will be split into two groups of five talents and work as a team.

At the end of the day, shortly before the Apéro riche, the young cyber talents will come on stage for the award ceremony. Meet the Future Cyber Talents!

Cyber Security Austria

The winning team at Swiss Cyber Storm Challenge will travel to the Alpen Security Challenge 2013 in Linz (Austria). The Austrians are doing the same; playing the online qualifications, finding the most talented Austrian cyber talents who will then fight aginst the Swiss team at the IKT conference in Linz (5-7. November 2013).

www.verbotengut.at



Conference Speaker Line-Up

Michael Anti (a.k.a. ZHOA Jing) - Blogger, China

Michael Anti (a.k.a. ZHAO Jing) is a veteran journalist and popular political columnist for various of Chinese and English media outlets. He won M100 Sanssouci Media Award in 2011. He was a Chinese war reporter in Baghdad in March 2003 and then worked with Beijing Bureau of the New York Times for 4 years.

His well-known MSN blog on Chinese politics was removed by Microsoft in December 2005 under the pressure of Chinese government. He also received Wolfson Press Fellowship at Cambridge University (2007), Nieman Fellowship at Harvard University (2008), and was a visiting scholar at University of Tokyo. As a public advocate for Internet freedom and online public diplomacy, he is one of the most influence bloggers in China. He was also a TEDGlobal speaker in 2012.

Candit Wüest - Symantec, Switzerland

Candid Wüest holds a master of computer science from the Swiss Federal Institute of Technology (ETH) and various certifications. He works for Symantecs global security response team, where he has been going far beyond anti virus signatures during the last ten years. He researches new threat vectors, analyses trends and formulates new mitigation strategies. During three years he was working as a Virus Analyst in the anti malware laboratory of Symantec in Dublin/Ireland, analysing malware and creating signatures. He has published various articles and appeared in magazines and TV shows. He is a frequent speaker at conferences like VB, RSA and #days. He learned coding and the English language on a Commodore 64.

Dr. Thomas Maillart - Swiss National Science Foundation Fellow, UC Berkeley School of Information, California, USA

Thomas Maillart has a PhD in Science from the Department of Management, Technology and Economics, ETH Zurich and a Master Degree in Engineering from EPFL. He is currently a Swiss National Science Foundation Fellow at UC Berkeley School of Information, developing scientific methods to model and forecast the dynamics of Internet attacks at large scales. Thomas is well known in the (re)insurance business for having demonstrated the extreme nature of cyber risks in 2008.

Conference Speaker Line-Up

John Matherly - Founder of Shodan

John Matherly is the founder of Shodan, the first comprehensive search engine of devices connected to the Internet. John, born in Switzerland, graduated from University of California, San Diego, with a bachelors degree in bioinformatics, with research done in the field of hydrogen-deuterium exchange mass spectrometry. Prior to creating Shodan, John worked at the San Diego Supercomputer Center as a programmer/analyst on the Protein Data Bank project. The idea of Shodan was born in 2003, and it has evolved into a tool that searches for and catalogs every IP address on the Internet, ranging from individual home desktops to industrial automation systems. Shodan also performs automatic Internet-wide surveys, analyzes large amounts of data and makes security tools more accessible to the community.

Dr. Timo Steffens - Vice Head National IT Situation Center and CERT-Bund, BSI

Timo Steffens has a background on artificial intelligence and data analysis. After doing projects on early-warning systems he found his way into the field of IT-security. He is the vice head of the National IT-Situation Center and CERT-Bund at the German Federal Office for Information Security (BSI).

Dr. Stefanie Frey - Reporting and Analysis Center for Information Assurance (MELANI)

Stefanie Frey has a PhD from the Department of War Studies, King's College London. She worked on several projects on defence and security policy, war related topics, current affairs, as well as early warning and crisis management. She is currently working on Cyber Risk and Defence at the Reporting and Analysis Centre for Information Assurance (MELANI) at the Federal Department of Finance FDF.

Conference Speaker Line-Up

Yaron Blachman - Security and Forensics Technology Leader, PwC Israel

Yaron Leads PwC Israels Security and Forensics line of services. He founded PwCs Cyber Center of Excellence and has an overall responsibility on its global operations. Yaron started working with the PwC security consulting group in 2002 where he has been providing security consulting services to the fortune 500 clients. Yaron has a great deal of experience in the financial sector, working with major banks and insurance companies - globally and in Israel. Prior to working with PwC, Yaron has been working as an IT consultant with Paragon Consulting (Israel) and has been a captain in the Israeli Air-Force, managing large scale IT software projects. Yaron is an electrical and computer engineer (Ben-Gurion University) and is a Certified Information System Security Professional (CISSP) since 2002.

Dr. Michael Pilgermann - Technical Advisor, Federal Ministry of the Interior, Germany

Michael Pilgermann has a doctorate in Computer Science with focus on Information Security. He had worked in industry for several years as an IT-Security consultant. In his current position as a technical advisor in the Federal Ministry of the Interior (MoI) he is taking care of the national and international CIIP activities and the European Union aspects of Cybersecurity/NIS.

Oliver Münchow - Senior Security Consultant, InfoGuard AG

Oliver Münchow works as a Senior Security Consultant at InfoGuard AG. He has a background of over ten years' experience in Penetration Testing, Security Audits and Vulnerability Assessment. He studied information security at the Lucerne University of Applied Sciences and Arts. Oliver achieved his Lic. Rer. Pol. (summa cum laude) at University of Fribourg.

Conference Speaker Line-Up

Manuel Krucker - Senior Security Consultant, InfoGuard AG

Manuel Krucker works as Senior Security Consultant at InfoGuard AG. He is an experienced Security Analyst holding a Master of Science in Computer Science ETH Zürich and is a certified OSSTMM Professional Security Analyst and Tester.

Dr. Stefan Lüders - CSO, CERN

Stefan Lüders, PhD, graduated from the Swiss Federal Institute of Technology in Zurich and joined CERN in 2002. Being initially developer of a common safety system used in all four experiments at the Large Hadron Collider, he gathered expertise in cyber-security issues of control systems. Consequently in 2004, he took over responsibilities in securing CERN's accelerator and infrastructure control systems against cyber-threats. Subsequently, he joined the CERN Computer Security Incident Response Team and is today heading this team as CERN's Computer Security Officer with the mandate to coordinate all aspects of CERN's computer security (office computing security, computer centre security, GRID computing security and control system security) whilst taking into account CERN's operational needs. Dr. Lüders has presented on these topics at many different occasions to international bodies, governments, and companies, and published several articles.

CYBER ATTACKS AND DEFENSE
SWISS CYBER STORM
WWW.SWISSCYBERSTORM.COM

www.swisscyberstorm.com

Meet the Future Cyber Talents

Gold Sponsor

Steigende Anzahl Cyber Angriffe auf produzierendes Gewerbe

Die Ergebnisse des neuen Symantec Sicherheitsreport lassen keinen Zweifel: Das produzierende Gewerbe ist das neue Top-Ziel für Hacker-Angriffe. Mit 24 Prozent aller gezielten Attacken im Jahr 2012 löste das produzierende Gewerbe Behörden und Regierungen als attraktivstes Ziel ab – die Tendenzen von 2011 haben sich damit fortgesetzt. Doch wieso greifen Hacker Industrieanlagen vermehrt an? Die meisten Attacken sind eindeutig wirtschaftlich oder politisch motiviert. Hier geht es darum, die Integrität von Produktionsabläufen und Produkten zu sabotieren. Allerdings ist diese Tatsache in vielen Unternehmen noch nicht angekommen.

Der Grund dafür: In der Vergangenheit waren solche gezielten Angriffe nur schwer möglich, da Industrieanlagen isolierte Systeme waren. Mit zunehmender Integration in das Unternehmensnetzwerk und dem Einsatz von Standard-Software wurden Produktionsstätten angreifbarer – eine Tatsache, die Hackern nicht verborgen blieb. Viele Firmen verfügen jedoch (noch) nicht über eine umfassende Sicherheitsstrategie, sondern halten schon die Implementierung einer Anti-Virus-Software oder einer Firewall für ausreichend. Dabei werden die Attacken immer ausgefeilter und erfordern ein holistisches Sicherheitssystem, das aus verschiedenen Komponenten besteht. Je nach Anforderung der Produktionsstätte gehören dazu Verschlüsselungs- und Authentifizierungstechnologien, Firewalls, Intrusion Prevention Lösungen oder Gateways.

Ein Beispiel ist die Automobilbranche, in der die Integrität der produzierten Bauteile und Fahrzeuge extrem wichtig ist. Gleichzeitig ist die Branche äusserst attraktiv für Hacker: Modelle und Entwürfe werden Jahre vor Marktreife entwickelt, Angriffe auf geistiges Eigentum lohnen sich besonders. Und auch beim Thema Spam schaffen es die Hersteller und Zulieferer in die unrühmlichen „Top Ten" auf den vierten Rang. Hier besteht Handlungsbedarf – sowohl beim Thema Sicherheitsstrategie als auch bei der Implementierung passender Komponenten.

Der Faktor Mensch sollte ebenfalls nicht unterschätzt werden. Die meisten Mitarbeiter gefährden die Sicherheit nicht böswillig, sondern schlicht aus Unwissenheit. Hier sind Schulungen notwendig, wie sich Sicherheitsrichtlinien einhalten lassen und welche Verhaltensweisen diese untergraben würden. So kann es zum Beispiel schon die Sicherheit gefährden, wenn die Urlaubsfotos auf dem USB-Stick über das Display des Schweissroboters angeschaut werden.

Das produzierende Gewerbe hat in den letzten Jahren bereits Fortschritte zur Absicherung seiner Anlagen gemacht. Doch das Tempo, in dem Sicherheitsstrategien entwickelt und Systeme implementiert werden, hält noch nicht mit den stets raffinierter werdenden Attacken Schritt. Dies erfordert auch ein Umdenken im Hinblick auf monetäre und personelle Investitionen, die sich mittelfristig auszahlen und zum Garant für wettbewerbsfähige Unternehmen werden.

Symantec Switzerland AG
Schaffhauserstr.134
8152 Glattbrugg

Tel: 044 305 72 00
E-Mail: info@symantec-events.ch
Internet: www.symantec.ch

Silver Sponsors

Dediziertes Hosting für geschäftskritische Anwendungen

aspectra ist ein führender Schweizer Anbieter für Application Outsourcing. Das KMU mit Sitz in Zürich übernimmt für seine Kunden den sicheren Betrieb von Systemen und Applikationen und garantiert mit zwei Rechenzentren höchste Verfügbarkeit. aspectra beschäftigt 23 Mitarbeitende, wovon die Mehrheit über einen Hochschulabschluss verfügt. Die Ingenieure betreuen entweder Microsoft oder Linux/Unix-Umgebungen und sind für ihre Fachgebiete zertifiziert (Microsoft, VMware, Citrix, RSA, Oracle, Linux etc.). Das Unternehmen erfüllt die Outsourcing-Anforderungen nach FINMA-RS 08/7 und ist ISO 27001 zertifiziert.

Kunden von aspectra sind unter anderen: Zürich Versicherung, SWICA, Basler Kantonalbank, Luzerner Kantonalbank, Hyposwiss, Suva, Reka, Gebäudeversicherung des Kantons Bern, Ex Libris, Unilever, Migros, Orell Füssli Wirtschaftsinformationen, Homegate, Jobwinner und alpha, NetMetrix, Staatskanzlei und Steueramt des Kantons Zürich, die Direktion für Entwicklung und Zusammenarbeit (DEZA).

IT Security Concepts and Projects

TEMET AG is a privately owned IT Security consulting company located in Zurich, Switzerland. It provides vendor independent consulting services in the areas of Security Management and Security Solutions, with a focus on Identity and Access Management (IAM) infrastructure projects.

Our consultants have a background in engineering and project management, and they are experienced practitioners. With this combination of skills, they can plan, guide and support even your most complex security initiatives. From the sketch book to production – we make your IT Security infrastructure work!

TEMET AG was founded 2010 by experienced IT Security professionals and currently employs eight consultants. Its customer base comprises more than 25 financial institutions and public authorities in Switzerland.

Silver Sponsors

pwc

Security is a core task of governments and an important social theme. Threats range from natural disasters and pandemics to terrorist attacks, organized crime and cybercrime. Enhancing security requires knowledge of the possible threats, knowledge of risks and knowledge about how to increase protection.

As a consequence of the complexity and openness of our societies, (national) security organizations cannot operate in isolation. Good cooperation between public sector organizations and the active participation of citizens and businesses is essential for an effective and agile provision of security. National and international security are closely related and security increasingly depends on good cooperation between national and international organizations.

PwC can help governments and corporations to better respond to the challenges they face. With every engagement we bring a fresh PwC experience to our clients as the #1 firm in professional services. With over 12,500 professionals in more than 150 countries, we can improve performance in governments, markets, institutions and international governmental organizations.

Partners

Amt für Informatik und Organisation

POLICE

swisscom

Contributors

- Digicomp AG, Zürich
- netnea ag, Bern-Liebefeld
- TerreActive AG, Aarau

Cyber Challenge Provider

COMPASS SECURITY

Compass Security is providing the Hacking-Lab system for the Swiss and Austrian cyber competition.

www.hacking-lab.com

Thank You

I hope you have utilized this opportunity to gather and exchange information and for networking purposes. Perhaps you were able to discover a product or a new solution to make your daily duties easier during a conversation with one of our sponsors? Perhaps you took the opportunity to speak with one or more of the young talents? Or maybe you have even invited these young prospects to visit your company?

In short: I hope to welcome you at the Swiss Cyber Storm 5 Conference next year.

We are happy to consider your ideas and suggestions for improvements at ok@swisscyberstorm.com. We depend on your suggestions: After all, we want to create an event for YOU. If you are interested in participating in the organisation or would like to become a sponsor please contact me at president@swisscyberstorm.com

Acknowledgements

I would like to take this opportunity to extend a special thank you to everyone that made Swiss Cyber Storm possible. In addition to the conference participants, this also includes our patrons, the reporting- and analysis office for information security MELANIE and Swiss Police ICT (SPIK). Their support opened numerous doors, which ordinarily would have remained closed. I would also like to thank our Gold Sponsor Symantec, as well as all other sponsors. Without their commitment, events with foreign experts and events for professional exchange and networking in a volume of Swiss Cyber Storm 4 would have difficult, if not impossible to organize at a moderate cost.

In connection with the Security Alpen Cup, I would also like to thank the judges for their professional competency and support during the evaluation of the young talents. A special thank you to the Compass Security AG, and/or their Hacking-Lab for providing the infrastructure and the tasks for the security challenges.

Finally, I would also like to thank the OK members and all other individuals who voluntarily helped with the Swiss Cyber Storm 4 with great commitment.

President Swiss Cyber Storm Association

Bernhard Tellenbach

president@swisscyberstorm.com

https://www.swisscyberstorm.com