



Editorial

Neue Vorstandsmitglieder, neue Fachvideos und zertifizierte Website

Als neu gewählte Vizepräsidentin bedanke ich mich vorab bei denjenigen, die mir an der Generalversammlung die Stimme gegeben haben und begrüsse Sie alle ganz herzlich. Voller Energie und mit viel Freude werde ich mich für ISSS einsetzen.

Sollten Sie einen unserer Security Lunches oder eine Abendveranstaltung verpasst haben, können Sie sich im ISSSview Videoportal die entsprechenden Aufzeichnungen, insbesondere der zwei letzten Security Lunches und der Veranstaltung „Informationsschutz im Zeitalter von Wikileaks“, welche auf grosse Resonanz gestossen sind, ansehen.

Ich lade Sie ein, unsere Website <http://www.issss.ch> zu besuchen. Seit Mitte März verfügt ISSS über ein von Verisign zur Verfügung gestelltes Standard Extended Validation SSL Certificate, womit unsere Website nun im Browser als zertifiziert ausgewiesen wird. ISSS diskutiert nicht nur Security, wir leben sie auch.

Dr. Ursula Widmer
Vizepräsidentin, ISSS
vicepresident@issss.ch

Highlights in dieser Ausgabe

ISSS:

- Zertifizierte ISSS-Website
- Neue Verstärkung für den ISSS-Vorstand
- Neue Partnerschaften

GV:

- Wahlergebnisse
- Votingfragen

Review:

- Security Lunch mit Luzius Meisser
- Abendveranstaltung WikiLeaks
- 2. ISSS St. Galler Tagung

Agenda:

- ISSS Zürcher Tagung 2011
- Partner Events
- ISSS Events

ISSS Kurznews

Zertifizierte ISSS-Website

Die Website <https://www.issss.ch/> verwendet seit Mitte März 2011 ein Standard Extended Validation SSL Certificate von Verisign. Dieses wird in den verschiedenen Web Browser speziell mit grüner Farbe hervorgehoben. Verisign, eine Tochterfirma von Symantec, hat uns das Zertifikat gratis ausgestellt, wofür wir uns bedanken.



ISSSview Neuzugänge

Auf unserem Videoportal finden Sie seit Mitte Februar zusätzliche Aufzeichnungen zu diversen ISSS Veranstaltungen:

Security Lunch vom 10.02.2011 von Luzius Meisser
„Cloud Storage Security“
<http://www.youtube.com/watch?v=I38G6YWJKDE>



Security Lunch vom 08.03.2011 von Candid Wüest
„Technische Einblicke in moderne Anti-Viren Software“
<http://www.youtube.com/watch?v=nTI2EpdEZdo>



Abendveranstaltung „Informationsschutz im Zeitalter von Wikileaks“

- Begrüssung durch ISSS <http://www.youtube.com/watch?v=bP60NjEGMZk>
- „Wikileaks im Recht“ <http://www.youtube.com/watch?v=jkeyp0HICqY>
- Fachstatements von Experten <http://www.youtube.com/watch?v=UI5wgeNONBY>
- Podiumsdiskussion <http://www.youtube.com/watch?v=T7x-591oxfc>



Review: ISSS Generalversammlung 2011



Das detaillierte Protokoll sowie weitere Unterlagen zur ISSS Generalversammlung 2011 finden interessierte Mitglieder im Memberbereich der ISSS-Website: <https://www.iss.ch/mitgliederbereich/>

Review: Security Lunch

„Cloud Storage Security“ von Luzius Meisser

Autor: Luzius Meisser



Beim ISSS Security Lunch vom 10.2.2011 hat Luzius Meisser, Mitgründer von Wuala, zum Thema Cloud Storage Security gesprochen. Das Referat führte durch verschiedene Ansätze, Si-

cherheit bei Cloud Storage Systemen zu erreichen. Diese Ansätze wurden in zwei Kategorien eingeteilt: Ansätze mit oberflächlicher und solche mit system-immanenter Sicherheit. System-immanente Sicherheit bedeutet, dass die Sicherheit intrinsisch, also Teil des Designs und tief im System verankert ist. Einerseits schränkt dies die Freiheiten ein, die man als Benutzer oder Entwickler hat, andererseits verhilft dies einem aber auch zu enorm starken Sicherheitsgarantien.

Als Beispiel für oberflächliche Sicherheit diene Windows 95, bei dem die Sicherheit erst später aufgesetzt wurde und deshalb nicht im System verankert ist, was zahlreiche Sicherheitsprobleme zur Folge hatte. Ein weiteres Beispiel für eher oberflächliche Sicherheit bietet Facebook, wessen produktive Datenbank sämtlichen Entwicklern zugänglich ist. Zudem wird zwar https unterstützt, der Standard ist aber eine unverschlüsselte Verbindung.

Der erste Schritt, die Sicherheit eines Web-Dienstes zu erhöhen, besteht normalerweise darin, die Verbindung zu verschlüsseln. Geht es um sensitive Daten, werden zum Teil auch die abgelegten Daten verschlüsselt und der Zugang zu den Datenbanken betriebsintern eingeschränkt. Der Betreiber eines solchen Dienstes hat aber immer noch Zugriff auf die Daten und kann zum Beispiel, wie es unlängst Twitter passiert ist, von einer Regierung gezwungen werden, Benutzerdaten herauszugeben. Des Weiteren schützt diese Art von Sicherheit

nur beschränkt vor Hacker-Angriffen, Programmierfehlern und Social Engineering. Als Beispiel wurde SourceForge genannt, welches im Januar sämtliche Passwörter seine Benutzer zurückgesetzt hat, nachdem man Hinweise auf einen möglicherweise erfolgreichen Angriff gefunden hatte.

Einen Weg, diese Art der Angriffe systematisch zu verhindern, besteht darin, sämtliche Daten client-seitig zu verschlüsseln. Sämtliche Daten werden auf dem Computer des Benutzers verschlüsselt, bevor sie hochgeladen werden. In einem solchen Szenario kann ein Hacker im Worst-Case zwar noch alle Daten löschen, doch er kann sich nicht Zugang dazu verschaffen, selbst wenn er physischen Zugang zu den Servern hat, welche die Daten beherbergen. Gleichzeitig wird auch die Lage für den Betreiber angenehmer, da sich die Frage, ob und wie er auf allfällige rechtliche Anfragen nach der Herausgabe von Daten reagieren soll, gar nicht mehr stellt. Es gibt zahlreiche rechtliche Wege, jemanden zur Herausgabe von Daten zu zwingen. Es gibt aber sehr wenige Möglichkeiten, einen Betreiber eines Services dazu zu zwingen, seine Benutzer zu überwachen und Daten zu sammeln. Somit kann system-immanente Sicherheit dabei helfen, Daten vor rechtlichen Risiken zu schützen. Dies hat den grossen Vorteil, dass viel mehr Freiheiten in der Wahl des Standorts und des Anbieters von Cloud-Infrastruktur besteht. So kann zum Beispiel die Sicherheit der Daten auch dann noch gewährleistet werden, wenn das Rechenzentrum keine entsprechende Zertifizierungen besitzt und vertraglich keine Sicherheit garantiert. Auch wird es zum Teil möglich, Daten im Ausland zu speichern, die von Gesetzeswegen Ausländern nicht zugänglich gemacht werden dürfen.

Review: Security Lunch

Der fundamentale Vorteil der client-seitigen Verschlüsselung, nämlich dass der Anbieter des Datenspeichers keinen Zugang zu den Daten hat, ist auch gleichzeitig ihre Achilles-Ferse. Damit wird nämlich nicht nur der Zugang zur aus Sicht des Datenbesitzers illegitimen Zwecken, sondern auch der Zugang zu legitimen Zwecken verhindert. Es wird sehr viel schwieriger, die gespeicherten Daten serverseitig zu analysieren und zu pflegen. Es ist nicht möglich, einen zentralisierten Suchindex aufzubauen. Und wenn der Benutzer sein Passwort vergisst, sind die gespeicherten Daten für immer verloren. Dies ist übrigens oft der effizienteste Weg, herauszufinden, ob ein Service tatsächlich sicher ist und die Daten client-seitig verschlüsselt. Anstatt im Kleingedruckten technischer zu suchen, wie nun genau 'encrypted storage' gemeint ist, kann man auch überprüfen, ob ein Service eine 'password recovery/reset' Funktion anbietet. Falls eine solche existiert, hat der Anbieter Zugang zu den Daten seiner Kunden. Falls nicht, ist das ein starkes Indiz dafür, dass die Daten tatsächlich client-seitig verschlüsselt werden.

Es gibt einige Backup-Services, die client-seitige Verschlüsselung zumindest als Option anbieten. Sind aber Services über das reine Backup hinaus erwünscht, gibt es aufgrund der erwähnten technischen Einschränkungen, kaum mehr sicher verschlüsselte Services. Beispi-

le für gut verschlüsselte Speicher-Anbieter sind SpiderOak und das von Luzius Meisser gegründete Wuala. In letzterem wird das Teilen von Ordnern mittels Cryptree ermöglicht, einem Schlüssel-Management-System, welches Luzius als Teil seiner Master-Arbeit an der ETH entwickelt hat und dessen Grundbausteine im Talk kurz beschrieben wurden.

Abgeschlossen hat der Talk mit einer Exkursion zu zwei Möglichkeiten, die Einschränkungen von client-seitiger Verschlüsselung zu verkleinern. Die eine nennt sich 'full homomorphic encryption' und versucht, mit cleveren Algorithmen Berechnungen auf verschlüsselten Daten auszuführen, was bislang aber nicht praktikabel ist und in absehbarer Zeit auch nicht sein wird. Die andere besteht in einem hybriden Ansatz, der darin besteht, die client-seitige Verschlüsselung dort anzuwenden, wo man von den Vorteilen wie günstige Infrastruktur profitieren kann, während es innerhalb des gleichen Services auch Teile geben kann (z.B. den Suchindex), der separat mit erhöhten Sicherheitsvorkehrungen betrieben wird.

Die 62-Prezi-Slides waren schon nach einer knappen halben Stunde durch und es folgten diverse Fragen und eine angeregte Diskussion rund um Wuala und Cloud Storage Security.

Bilder, Video und Präsentation des Security Lunches finden Sie unter <https://www.iss.ch/veranstaltungen/2011/security-lunch-2011-02-10/>

Review: ISSS Abendveranstaltung WikiLeaks

„Informationsschutz im Zeitalter von WikiLeaks“



http://blog.windfluechter.net/content/bl_1

Am Dienstag den 22. März 2011 fand im Hotel Novotel in Zürich die Abendveranstaltung zum aktuellen und hochbrisanten Thema „Informationsschutz im Zeitalter von WikiLeaks“ statt, welche von 87 Personen besucht wurde.

Eine treffende Definition von „WikiLeaks“ lieferte Prof. em. Dr. iur. Franz Riklin, Experte für Datenschutz, Medienrecht und Strafrecht. Er umschrieb „WikiLeaks“ als eine Online-Plattform, an welche Dritte Informationen über ein als unethisch oder rechtswidrig erachtetes Verhalten von Unternehmen oder staatlichen Organen, die bisher aufgrund von Geheimhaltung, Unterdrückung oder Zensur nicht allgemein zugänglich waren, zur weltweiten Verbreitung

über das Internet eingeben können, wobei sich die Betreiber der Webseite zur Wahrung der Anonymität der Hinweisgeber (sog. „Whistleblower“) verpflichten.

Nach der Eröffnungsrede durch Prof. Riklin wurde das Thema aus verschiedenen Werten beleuchtet: Die Bedeutung der Verfügbarkeit von Informationen für den Bürger kam ebenso zur Sprache wie Korruptionsbekämpfung dank „WikiLeaks“ und Möglichkeiten und Grenzen von Ermittlungen bei Information Leaks. Hanspeter Thür (Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter) Eric Guyer (Redaktor NZZ), Zora Ledergerber (Transparency International Schweiz), Felix Ceccato (BKP) und Crispin Tschirky von der Firma E3 stellten sich abschliessend einer angeregten Podiumsdiskussion, bei der auch das Publikum breit zu Wort kam.

Die Links zu den Videos finden Sie in der Rubrik „ISSS-view Neuzugänge“. Die komplette Präsentation steht auf der Eventwebseite zum Download bereit:

<https://www.iss.ch/veranstaltungen/2011/informationsschutz/>.

Review: ISSS 2. St. Galler Tagung

„2. ISSS St. Galler Tagung“

Autor: Lukas Ruf, Co-Organisator

Was sind Advanced Persistent Threats wirklich? Wie funktioniert ein modernes kriminelles Netzwerk? Hat die träge Politik überhaupt eine Chance, vor solchen Herausforderungen zu bestehen und die Gesellschaft auch im Cyberspace zu schützen? Diesen Fragen ging die 2. St. Galler Tagung der ISSS nach.

Am 5. April 2011 fand die zweite St. Galler Tagung der ISSS im Hotel Radisson Blu in St. Gallen statt, die vom ISSS Vorstand Ivan Bütler mit Lukas Ruf als Co-Organisator auf die Beine gestellt wurde. Thema der Veranstaltung war *Cyberspionage bei Firmen und Behörden – Erfahrungsberichte und Empfehlungen im Umgang mit der Gefahr von "Advanced Persistent Threat"*. Rund 60 Teilnehmer aus unterschiedlichsten Firmen, Behörden und Universitäten fanden den Weg und konnten am sehr spannenden Programm teilhaben.

Das Programm beinhaltete vier Vorträge zum Thema Cyberspionage und Advanced Persistent Threats, die durch kurze Pausen zum intensiven Austausch unter den Teilnehmern aufgelockert wurden. Ivan Bütler führte gekonnt durch das Programm und fand die treffenden Worte, die jeweiligen Referenten kurz vorzustellen.

Lukas Ruf führte als erster Referent in das Thema ein. Mit seinem Vortrag *Advanced Persistent Threat – Buzzword oder Realität* zeigte er mit einem systematischen Vorgehen auf, welche Aspekte eine Bedrohung zu einer fortschrittlichen Bedrohung werden lassen. Dabei betrachtete er die verschiedenen, im Web öffentlich auffindbaren Definitionen und beleuchtete die wesentlichen Aspekte. Aus diesen kristallisierte er die wesentlichen Eigenschaften, welche für die Klassifizierung entscheidend sind. Beispiele illustrierten die Betrachtungen und dienten dazu, das Thema in einen aktuellen Kontext zu rücken.

Mauro Vignatti schloss an die Einführungen an und zeigte in seinem Vortrag *Modern Criminal Networks: Infrastructure and Tasks Segmentation of Today's Criminal Groups*



in Cyberspace auf, wie sich heute internationale, kriminelle Netzwerke im Internet abbilden. Die spannende Darstellung der strengen Strukturen, die den Chef eines Netzwerks vor den Verfolgern durch Proxies schützen, lässt nur erahnen, wie herausfordernd die Zukunft der Cyber-Security sein wird.

Mark Saxer ging unter dem Titel *„Gibt es öffentliche Sicherheit im Cyberspace?“* auf die Herausforderungen ein, die der Cyberspace für die Politik und die nationale sowie öffentliche Sicherheit bereithält. Er zeichnete die Geschichte der entsprechenden parlamentarischen Vorstösse nach und zeigte unter anderem auf, dass die Themen Cybercrime und Cyberwar statistisch gesehen von der CVP und der SP dominiert werden – und, zumindest hochgerechnet, von Frauen. Anhand diverser Beispiele illustrierte er die Schwierigkeiten, parlamentarische Begehren zu diesen Themen zum Erfolg zu führen. Allerdings aber habe der Bundesrat Ende 2010 – nach 10 Jahren Druck – einen Projektleiter Cyber Defense ernannt, der bis Ende 2011 eine Strategie vorlegen werde. Saxer betonte sein volles Vertrauen in das Projekt: Die ganze Herangehensweise sei ausserordentlich systematisch und durchdacht.

SOPHOS
und **utimaco**

Die Firma Sophos AG unterstützte die 2. St. Galler Tagung als Hauptsponsor. In ihrem Referat stellte sie ihre Schutz-Suite für mobile Geräte vor, mit deren Hilfe Smartphones kontrolliert in Unternehmensnetze eingebunden werden können.

Abgeschlossen wurde die sehr erfolgreiche Veranstaltung mit Dankesworten unseres Präsidenten, Thomas Dübendorfer, die zu einem lukullischen Apéro übergeleitet haben. Dieser bot Gelegenheit, das Gehörte mit Gleichgesinnten in Diskussionen zu besprechen ebenso wie bei den Referenten Rückfragen vorzunehmen. Freuen wir uns auf die 3. St. Galler Tagung im 2012.



Partnerschaften mit ISSS

Wir freuen uns, Ihnen hier unsere beiden neuen Partner, Dreamlab Technologies AG und TeleTrust, genauer vorzustellen.

Dreamlab Technologies AG – Security is our passion

Dreamlab Technologies AG ist ein international tätiger Schweizer IT-Security Provider. Als Member of the Board von ISECOM, sowie W3C- und OWASP-Mitglied ist es Dreamlab ein Anliegen das breite Fachwissen dem IT-Nachwuchs zugänglich zu machen.

Aus diesem Grund engagiert sich Dreamlab auch an diversen Fachhochschulen an denen ihre Mitarbeiter als Trainer den Studenten in verschiedenen Studiengängen ihr Fachwissen zugänglich machen.

Kernstück dabei bilden die OSSTMM Kurse von ISECOM, an deren Entwicklung Dreamlab massgeblich beteiligt ist. Das OSSTMM ist heute die weltweit erfolgreichste Methodik für Systemaudits und wurde erst kürzlich in der Version 3.0 der breiten Öffentlichkeit zugänglich gemacht.

TeleTrust Deutschland e. V.

Der IT-Sicherheitsverband TeleTrust Deutschland e.V. wurde 1989 gegründet, um verlässliche Rahmenbedingungen für den vertrauenswürdigen Einsatz von Informations- und Kommunikationstechnik zu schaffen. TeleTrust entwickelte sich zu einem bekannten Kompetenznetzwerk für IT-Sicherheit. Heute umfasst TeleTrust mehr als 100 Mitglieder aus Industrie, Wissenschaft, Forschung und öffentlichen Institutionen sowie Partnerorganisationen aus Deutschland und Europa. In Projektgruppen zu aktuellen Fragestellungen der IT-Sicherheit und des Sicherheitsmanagements tauschen die Mitglieder ihr Know-how aus. TeleTrust äußert sich zu politischen und rechtlichen Fragen, organisiert Veranstaltungen und Veranstaltungsbeteiligungen und ist Träger der "European Bridge CA" (Beitstellung von Public-Key-Zertifikaten für sichere E-

Ein weiteres grosses Engagement von Dreamlab steckt in der Entwicklung von Certified Secure Web CSW. Die daraus resultierende Ausbildung zum Certified Secure Web Developer ist die hersteller- und technologieunabhängige Ausbildung für die Entwicklung sicherer Webapplikationen. Abgerundet wird dieses umfangreiche Schulungsangebot durch die Offensive Security Kurse basierend auf <<back | track.

<https://www.dreamlab.net/education>



Mailkommunikation) sowie des Zertifikates "TeleTrust Information Security Professional" (T.I.S.P.). Hauptsitz des Verbandes ist Berlin. TeleTrust ist Mitglied des European Telecommunications Standards Institute (ETSI).



Kontakt:
TeleTrust Deutschland e.V.
Dr. Holger Mühlbauer
Geschäftsführer
Chausseestraße 17
10115 Berlin
Tel.: +49 30 4005 4306
Fax: +49 30 4005 4311
<http://www.teletrust.de>

Agenda: ISSS Zürcher Tagung

"Soziale Netzwerke - Informationsquelle oder Risikoherd?"

Mittwoch, 8. Juni 2011 von 13.30 bis 18.00 Uhr im IBM Forum Zürich Altstetten

Anmeldung

<https://www.iss.ch/veranstaltungen/2011/zuercher-tagung/anmeldung/>

Die Entwicklung sozialer Netzwerke ist so weit fortgeschritten, dass Anwendungen und Einsatz im professionellen Bereich rasch zunehmen. Es entstehen neue Geschäftsmodelle, die einen Vorsprung im Wettbewerb verschaffen. Die Sperrung des Zugangs zu sozialen Netzwerken, wie sie von diversen Firmen und Behörden angeordnet wurde, kann die erkannten Sicherheitsprobleme auf die Dauer nicht lösen, weil die heutigen Informatikmittel den Angestellten Möglichkeiten zur Nutzung sozialer Netzwerke anbieten, die von den Firmen kaum kontrolliert werden können. Es ist daher vordringlich, gute, umfassende und umsetzbare Lösungen für die Nutzung sozialer Netzwerke in Unternehmen und Verwaltung zu entwickeln.

Wir freuen uns besonders, dass Isabelle Welton, CEO IBM Schweiz, an der Zürcher Tagung 2011 das Eröffnungsreferat halten wird. Anschliessend werden ausgewiesene Experten das juristische Umfeld sozialer Netzwerke darstellen und anhand konkreter Beispiele aus führenden Firmen organisatorisch-technische Lösungen für den Umgang mit sozialen Netzwerken aufzeigen. In Podiumsdiskussionen sollen die Chancen und Risiken sozialer Netzwerke kontrovers diskutiert als auch Teilnehmerfragen beantwortet werden.

Programm

13:00	Registrierung
13:30	Begrüssung zur Zürcher Tagung 2011 Keynote: Soziale Netzwerke - mehr als nur eine Informationsquelle Referentin: Isabelle Welton CEO, IBM Schweiz

Technischer/Organisatorischer Teil

Soziale Netzwerke - Vielschichtige Gefahren eines neuen Zeitalters
Referent: Marc Ruef, scip AG
Social Media und Security bei Siemens Schweiz AG
Referent: Roman Fischer, Information Security Officer, Siemens
Malware in Sozialen Netzwerken
Referent von Sophos AG

Juristischer Teil

	Rechtliche Herausforderung der Social Media Referent: Dr. Robert G. Briner, Rechtsanwalt Rechte und Pflichten der Arbeitnehmer beim Umgang mit den Social Media Referent: Dr. Adrian von Kaenel, Rechtsanwalt
18:00	Apéro

Weitere Details finden Sie unter <https://www.iss.ch/veranstaltungen/2011/zuercher-tagung/>

Goldsponsor

 SOPHOS
und utimaco

Agenda: Partner Events mit Rabatt für ISSS Mitglieder

Cyber Crime, Risk Resilience & Security Governance

What do the Next 5 Years Hold? How are Key Areas Maturing?

8 - 10 June 2011, Ergife Palace Hotel, Rome

Email: kbevan@mistieurope.com

Exclusive **15% Discount** for ISSS Members

Stay one step ahead of rapidly changing business environments, current cyber threats, strategies and responses at the [8th Annual CISO Summit & Roundtable, 8 - 10 June 2011](#) in Rome, Italy.

Attend to gain insights into crux questions: What will prove to have the biggest impact and long term effects on the information security profession and cyber risk field as a whole? How are your peers preparing for the future? How can you define today's and tomorrow's high value targets? Does the CISO job description really need to be re-written?

Rome 2011 promises to provide the most thoughtful discussions yet given **recent emerging security trends** and stories directly impacting the profession. It has been a busy period for cyber criminals. Take '**Operation Aurora**'; **Stuxnet**; **Zeus**; **iPad Info Hack**. Add to this **WikiLeaks**, ongoing social networking privacy debates, calls for new cyber security legislation...

Dynamic keynotes and unrivalled speaker panels:

Jim Reavis, Executive Director, **Cloud Security Alliance (USA)** - "**Cloud Security & The Future Of Information Security**"; **Don Randall**, MBE, Head of Security, **Bank of England** & Chairman of the '**Sister Banks**', the **City of London Crime Prevention Association** and '**Project Griffin** - "**Strategic Partnerships For Cyber Security: Identify, Prevent, Deter & Detect The Reality**"; **Nils Puhmann**, Co-Founder, **Cloud Security Alliance & CSO**, **Zynga**; **Dr. Simon Singh**, Best-Selling Author; Journalist, Radio Broadcaster, TV Producer and Director - "**The Science of Secrecy**"

Swiss Cyber Storm 3

Internationale IT Security Konferenz - 12. – 15. Mai 2011, Rapperswil

Drei parallele Tracks mit 36 Referenten aus USA, Europa und Asien zu den Themen

- Cyber Crime
- Exploit & Defense
- OWASP Web Security

Der Cyber Crime Track richtet sich an IT Sec Verantwortliche, CISO und Risk Manager. Die anderen zwei Tracks sind für IT Sec Engineers. Am Donnerstagabend findet der VIP Cruise auf dem Zürichsee statt mit allen Gästen und Referenten. Meet the Lead. Der 4-day Pass enthält den kostenlosen Zugang am Weekend, wo wir den besten IT Sec Experten suchen. Es gibt ein Auto im Wert von CHF 30'000 zu gewinnen.

Anmeldung: <https://www.swisscyberstorm.com/register/index.html> , Angabe von ISSS Mitgliedernummer im Kommentarfeld (Rabatt Gewährung für ISSS Mitglieder – 4day: CHF 950.- anstelle CHF 1'190.- und 2day: CHF 120.- anstelle CHF 150.-) Details: <http://media.hacking-lab.com/scs3/scs3details.pdf>

ISSE 2011 – Information Security Solutions Europe Conference

22 – 23 November 2011, Prague, Czech Republic

Call for Contributions

This call is intended to call for papers and other contributions such as round tables, panels and plenaries. Papers can be accepted for the ISSE Publication regardless whether they will be presented at ISSE 2011.

Topics: Public Cloud Challenges, Trustworthy Infrastructures, Mobile Security Solutions, Awareness and Education, to point out a few.

Concerning the submission, please contact Sophie Reimer, Programme Manager, sophie.reimer@teletrust.de

Deadline for Submission: April 21st 2011

For further information please follow the link <http://www.teletrust.de/veranstaltungen/isse/isse-2011/>

Agenda: Partner Events mit Rabatt für ISSS Mitglieder

Nächste Security Events unserer Partner

Programm und Anmeldung unter: <https://www.issss.ch/veranstaltungen/aktuell/>

Datum	Zeit	Veranstalter	Titel und Details	Ort
Di, 10.05.2011	10:30 - 13:30	BCMnet.ch	BCI Forum - Impact of Social Media on BCM What does it mean being prepared for a serious incident in the age of social media. free Details , Anmeldung	Neuchâtel
Do – So 12.05.- 15.05.2011	ganztags	Compass Security	Swiss Cyber Storm 3 Internationale IT Security Konferenz. Drei parallele Tracks mit 36 Referenten aus USA, Europa und Asien. 15% Rabatt für ISSS Mitglieder. Mitgliedernummer im Kommentarfeld angeben. Details , Anmeldung	Rapperswil
Fr, 20.05.2011	ganztags	TeleTrusT Deutschland e.V.	TeleTrusT-Informationstag "Cyber Crime" Überblick über die Cyber Crime-Gefahrenlage, angewendete Methoden und mögliche Schutzmaßnahmen Details , Anmeldung .	Berlin
Di - Mi 24.05.- 25.05.2011	ganztags	Vereon	IT-Notfallmanagement Sicherheit und Administrierbarkeit im Unternehmenseinsatz. 15% Rabatt für ISSS Mitglieder. Anmeldecode INM4128 angeben. Details , Anmeldung	Zürich

Digicomp Hacking Day 2011

Am 16. Juni veranstaltet ISSS zusammen mit Digicomp auch in diesem Jahr den Hacking Day. Acht Referate und Live-Demos beleuchten bei Digicomp Zürich die Thematik aus unterschiedlichen Perspektiven: Cyber Crime, Cloud Hacking, Audit und Forensic in virtuellen Umgebungen sind Schwerpunkte des Tagesprogramms. Die Agenda zur Selbstauswahl und Anmeldung ist ab sofort online: <http://www.digicomp.ch/hackingday>
Spezial-Konditionen: 15% Sonderrabatt für ISSS-Mitglieder. Als Rechnungsvermerk "ISSS-Mitglied" eingeben.

Nächste Security Kurse unserer Partner

Programm und Anmeldung unter: <https://www.issss.ch/veranstaltungen/kurse/>

Di - Mi 03.05.- 01.06.2011	09:00 - 17:30	Dreamlab Technologies	OSSTMM Professional Security Analyst OPSA DLCH-OPSA311SUI CHF 5300 Details , Anmeldung	Fribourg
Mo – Do 09.05.- 12.05.2011	09:00 - 17:30	OneConsult GmbH	OPSA (OSSTMM Professional Security Analyst) (ENGLISH) Course language: English (material: English) Details , Anmeldung	Thalwil
Mo – Fr 09.05.- 13.05.2011	10:00 - 16:00	Swiss Infosec AG	Betrieblicher Datenschutzverantwortlicher Wir führen Sie in die Aufgaben eines Datenschutzverantwortlichen ein und zeigen Problemstellungen aus der Praxis auf. CHF 4200.- Details	Zürich

Hier finden Sie weitere Events und Kurse unserer Partner: <http://www.issss.ch/veranstaltungen/veranstaltungen/>

Agenda: Partner Events mit Rabatt für ISSS Mitglieder

Nächste wissenschaftliche Konferenzen unserer Partner

Programm und Anmeldung unter <http://www.iss.ch/veranstaltungen/wiss-konferenzen/>

Di – Do 07.06.- 09.06.2011	ganztags	IFIP	IFIP SEC2011 - Future Challenges in Security and Privacy for Academia and Industry 15% Rabatt für ISSS Mitglieder Details , Anmeldung	Luzern
Di - Mi 20.09.- 21.09.2011	ganztags	GI et al.	D.A.CH Security 2011 Extended Abstract Submission bis 22.4.2011 Details , Anmeldung	Oldenburg, Deutschland
Di - Mi 22.11.- 23.11.2011	ganztags	Divers	ISSE 2011 Information Security Solutions Europe Conference Details	Prag, Tschechien

Agenda: Events der Information Security Society Switzerland

Nächste ISSS Fachtagungen

08.06.2011	13:30 - 19:00	ISSS Zürcher Tagung "Soziale Netzwerke - Informationsquelle oder Risikoherd?" (Anmeldung)	Zürich
24.11.2011	13:15 – 18:30	14. Berner Tagung für Informationssicherheit: Weitere Information folgen (Anmeldung)	Bern

Nächste ISSS Security Lunches

Eintritt kostenlos, auch für Nichtmitglieder; Essen wird zu Selbstkosten vom Restaurant vor Ort in bar eingezogen; **Anmeldung** erforderlich.

24.05.2011	12:00 – 14:00	Risk Management 2.0 (Anmeldung)	Zürich
------------	------------------	---	--------

Vollständige Agenda mit Links zu Programm und Anmeldung: www.iss.ch

Impressum

Information Security Society Switzerland

Wasserwerkstrasse 37

3000 Bern 13

newsflash@iss.ch

Tel. +41 31 311 5300

Auflage: Nur elektronische Auslieferung.

Versand als PDF per E-Mail an alle ISSS-Mitglieder und Publikation auf <http://www.iss.ch/>

