SBFI NEWS SEFRI

Informationen aus dem Staatssekretariat für Bildung, Forschung und Innovation SBFI

Juli / August 16

Staatskundeunterricht auf Sekundarstufe II

Swiss Cyber Risk Research Conference 2016

SHK Jahresbericht 2015

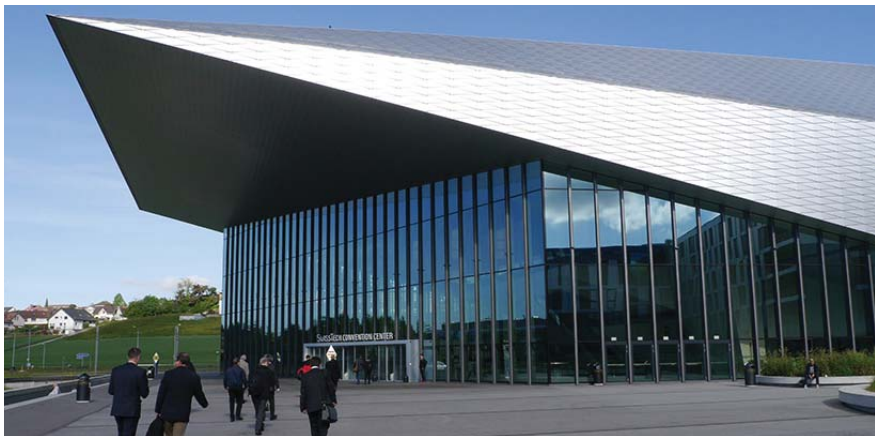
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Wirtschaft, Bildung und Forschung WBF
Staatssekretariat für Bildung, Forschung und Innovation SBFI

Erste Swiss Cyber Risk Research Conference 2016

Was kann gegen Cyber-Risiken unternommen werden?

Die Informations- und Kommunikationstechnologien entwickeln sich in Riesenschritten vorwärts. Kehrseite der Medaille sind Cyber-Risiken wie Blockierung von Systemen, Datendiebstahl oder Spionage. An der vom SBFI im Mai 2016 organisierten ersten Schweizer Cyber Risk Research Conference diskutierten an der ETH Lausanne über 300 Spezialistinnen und Spezialisten aus dem In- und Ausland darüber, wie man sich inskünftig besser vor Cyber-Risiken schützen kann.



Swiss Tech Convention Center, EPFL. Bilder: Christophe Stolz, SBFI

Der Bundesrat hat 2013 die «Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken» verabschiedet, mit der unser Land mittel- bis langfristig vor diesen neuen Gefahren geschützt werden soll. Dabei wurde das SBFI damit beauftragt, die Arbeiten zur Umsetzung der ersten von insgesamt 16 Massnahmen zu koordinieren. Diese erste Massnahme sieht vor, Forschung zur Identifikation von Cyber-Risiken zu betreiben.

Um diesen Auftrag zu erfüllen, wurde unter der Leitung des SBFI ein interdepartementaler Steuerungsausschuss aus Spezialistinnen und Spezialisten gebildet. Dieser schlug vor, eine Tagung zu organisieren, an der die Forschungsthemen in diesem Bereich vorgestellt werden, mit dem Ziel:

- Wechselbeziehungen innerhalb der Cyber-Risiko-Forschung in der Schweiz zu generieren,
- eine «Swiss Cyber Research Community» aufzubauen – eine Schweizer Cyber-Forschungsgemeinschaft also, die Forschende, Akademikerinnen und Akademiker sowie weitere Akteure im Bereich Cyber-Risiken in der Schweiz zusammenbringt –, und
- verschiedene Aspekte und Überlegungen zum Thema Schutz vor Cyber-Riken zu präsentieren, die dem weltweit höchsten Stand der Forschung entsprechen.

Die Organisatoren dieses Anlasses konnten auf die Teilnahme von hochrangigen Forschenden, Dozierenden und Vertreterinnen und Vertretern aus der Industrie zählen, die das Publikum an ihren reichen Erfahrungen teilhaben liessen. Sechzehn Referentinnen und Referenten beleuchteten das Thema aus ihrem jeweiligen Blickwinkel, brachten den Handlungsbedarf zur Sprache und zeigten Lösungswege auf.

Zum Abschluss der Konferenz zog Professor Martin Vetterli, Forschungsratspräsident des SNF und Spezialist für Kommunikationssysteme, ein klares Fazit: «In der Schweiz müssen wir in der IT und allgemein in den Computerwissenschaften an der Spitze bleiben, wenn wir die Cyber-Risiken im Griff haben wollen!»

Kontakt
Adrian Rohner, SBFI
Präsident interdepartementaler Steuerungsausschuss «Forschung und Bildung zum Schutz vor Cyber-Risiken»
☎ +41 58 463 01 79
✉ adrian.rohner@sbfi.admin.ch

Weitere Informationen
www.sbfi.admin.ch/cyber-risk

«Das Zeitalter der Quantentechnologie hat begonnen!»

Nicolas Gisin, Physikprofessor an der Universität Genf, hat eine höchst originelle Methode der Quantenkryptographie entwickelt, die unter anderem die Anerkennung des Massachusetts Institute of Technology MIT gefunden hat. Er erklärte den Teilnehmenden die potenziellen neuen Risiken der zukünftigen Quantencomputer und legte dar, wie man sich dank der Quantenkryptographie davor schützen kann.

Gisin stellte fest, dass es heute fast keine Zusammenarbeit zwischen Physikern und Kryptographen gibt und schlug deshalb vor:

- eine Gemeinschaft von Physikern und Kryptographen zu bilden, die gemeinsam an einer sicheren Quantenkryptographie arbeiten,
- geeignete Anwendungen für Quanten-Algorithmen zu identifizieren, beispielsweise für Mobiltelefone, für Anwendungen im öffentlichen Bereich oder zur Sicherung weiterer Bereiche des Online-Handels,
- geeignete Anwendungen für die Quantenkryptographie zu finden, beispielsweise durch die Installation einer Schweizer Quanten-Datenübertragungsleitung, dank der die Übertragung von Daten zwischen kritischen Infrastrukturen und grossen Rechenzentren gesichert werden kann.

«Absolutes Fehlen von Transparenz hat vorhersehbare Konsequenzen»

Virgil Dorin Gligor, Professor an der Carnegie Mellon University und bekannt für seine Forschungen über Informatiksicherheit, brachte mit seinem Referat mit dem provozierenden Titel «NSA: Teufel oder Sicherheitsbehörde für die Demokratie?» grundlegende Fragen zur Sprache.

Er erklärte anschaulich, mit welchen Schwierigkeiten ein staatlicher Nachrichtendienst konfrontiert ist. Insbesondere beschäftigte er sich mit der Frage, wie man im Cyberspace ausländischen Gegnern – Terroristen beispielsweise – «zuhören» kann, ohne gleichzeitig amerikanische Staatsangehörige zu belauschen. Wie kann man Letzteren glaubwürdig versichern, dass ihr eigener Nachrichtendienst sie nicht ausspioniert? Virgil Dorin Gligor hat die folgenden wichtigsten Lehren aus seiner Analyse gezogen:

- Das absolute Fehlen von staatlicher Transparenz, beispielsweise nie etwas sagen, führt oft zu falschen Mythen oder gar Verschwörungstheorien. Die rund ein Dutzend bekannten problematischen Fälle, in die die NSA verwikkelt ist, könnten letztlich zu einem Vertrauensverlust der Bürgerinnen und Bürger in ihre Regierung führen.
- Bei der Überprüfung von Abhörgenehmigungen müssen die zuständigen Gerichte in den Vereinigten Staaten alle Parteien auf neutrale Weise anhören und den Eindruck vermeiden, parteiisch zugunsten einer Regierungsbehörde zu entscheiden.
- Die Gesetze und die Politik der Vereinigten Staaten müssen an die neuen Technologien angepasst werden. Auch wenn sie über ein vertieftes Wissen verfügen, brauchen die Gerichte Unterstützung, um die neuen Technologien zu verstehen.

«Wir müssen die Reaktionsgeschwindigkeit auf allen Ebenen steigern»

Louis Marinos, Senior Expert bei der Europäischen Agentur für Netz- und Informationssicherheit (ENISA), eröffnete die Tagung mit der Präsentation einer Cyber-Bedrohungslandschaft. Er erläuterte, wie die verschiedenen Varianten aussehen, weshalb es schwierig ist, die Urheber einer Attacke eindeutig zu identifizieren und welche Massnahmen ergriffen werden können, um sich effizient gegen Angriffe zu verteidigen.

Der ausgewiesene Experte betonte, dass die Bedrohungsintelligenz der Schlüssel für alle Sektoren des Risikomanagements und der Managementsysteme für Informationssicherheit (ISMS) ist. Gleichzeitig müsse aber auch die Bildung des auf das Risikomanagement spezialisierten Personals verbessert werden, um schneller auf Angriffe reagieren zu können.
Abschliessend erklärte Louis Marinos, es sei notwendig:

- «angewandte statistische» Modelle zu entwickeln, um die Vergleichbarkeit von Informationen über Cyber-Bedrohungen und Vorfälle zu verbessern,
- neue Schutzmodelle zu entwickeln, die in komplexe, miteinander verbundene Endanwender-Umgebungen integriert werden können und einwandfreie Sicherheitskontrollen ermöglichen,
- leistungsstarke Computer-Modelle zu entwickeln, die die Bedrohungslandschaft simulieren können, so dass frühzeitig geeignete Schutzreaktionen getestet werden können,
- in ein besseres Management der Verwundbarkeiten und die Ausschöpfung des Darknets zu investieren.

«Kritische Infrastrukturen vor Cyber-Bedrohungen schützen»

Ralph Langner, renommierter deutscher Forscher, hat den Stuxnet-Virus entdeckt und analysiert, der die Zentrifugen in der iranischen Urananreicherungsanlage in Natans zum Erliegen brachte. Er ging auf die Möglichkeiten und Auswirkungen von Cyber-Angriffen ein.

Umfassende Cyber-Attacken auf physische Systeme sind keine Hacker-Angriffe:

- Sie können inakzeptable Auswirkungen auf die nationale Sicherheit eines Landes haben.
- Sie werden von Technikern auf Regierungsebene und nicht von Hackern geplant und ausgeführt.
- Ihr Ziel sind «schadhafte Manipulationen» an physischen Systemen.

Ralph Langner nannte eine Reihe von Beispielen, so etwa die vor Kurzem erfolgte Cyber-Attacke, mit der das ukrainische Stromversorgungsnetz lahmgelegt wurde. Ausserdem erinnerte er an die legendäre Schlagkraft des Stuxnet-Virus.

Langner erklärte, hochkomplexe digitale oder analoge Sicherheitssysteme könnten umgangen werden, um beispielsweise einen nuklearen Unfall zu verursachen und damit eine Umweltkatastrophe auszulösen.