

wirtschaftsforum spezial

ZENTRALSCHWEIZER
WIRTSCHAFTSFORUM 2018

ihz
INDUSTRIE- UND HANDELSKAMMER
ZENTRALSCHWEIZ

SPECIAL REVIEW ZUM 8. ZENTRALSCHWEIZER WIRTSCHAFTSFORUM

Mittwoch, 12. September 2018



Opening Key Notes:
**Politische Stabilität,
Standortfaktor und
Cyber Security**
Seiten 3-5

Workshops:
**Von Cyber Crime,
Gefahren-Management
bis Marktchancen**
Seiten 6-9

Closing Key Notes:
**NDB, Patrouille
Suisse und Bundesrat
Guy Parmelin**
Seiten 10-11

Impressionen vom Pilatus:
**Networking auf
2'132 M.ü.M.**
Seite 12

WIR MÜSSEN DEN GRUNDWERTEN UNSERES ERFOLGS SORGE TRAGEN!

Sicherheit, Vertrauen und Verlässlichkeit gehören zu den grossen Stärken der Schweiz. Sowohl auf institutioneller, politischer wie auch auf individueller Ebene.

Gerade in der heutigen Welt, die zunehmend unberechenbarer und immer stärker geprägt ist von Volatilität und Unsicherheiten, gehören Sicherheit, Vertrauen und Verlässlichkeit zum Rückgrat unseres wirtschaftlichen und gesellschaftlichen Erfolgs. Schon bei den einleitenden Worten des Präsidenten der IHZ, Andreas Ruch, wird jedoch klar, dass diese Werte zu erodieren und auch bei uns in den Hintergrund zu geraten drohen. So stellen zum Beispiel die Diskussionen um das Rahmenabkommen mit der EU oder um die Renten- und Steuerreform, aber auch die wirtschaftsschädlichen Initiativen zu Fair Food, Selbstbestimmung und Unternehmensverantwortung die Glaubwürdigkeit der Schweiz zunehmend in Frage.

Dass Sicherheit nicht nur als übergeordneter Standortfaktor seine Gültigkeit hat, sondern auch auf betriebswirtschaftlicher Ebene zu einem wichtigen Kostentreiber werden kann, zeigt Felix Howald, Direktor der IHZ, in seinen Begrüssungsworten auf, indem er auf seine Erfahrung in Lateinamerika verweist. Dort wird die fehlende Sicherheit immer unter den wichtigsten Faktoren genannt, wenn man Unternehmer nach ihren grössten Problemen fragt. Dabei handelt es sich nicht um Sicherheit in einem übergeordneten, eher abstrakten Sinne, sondern um ganz handfeste, konkrete Sicherheit: Sicherheit vor Überfällen, Entführungen, Diebstählen und Bedrohungen an Leib und Leben. Da haben wir in der Schweiz und ganz besonders in der Zentralschweiz noch ganz andere Herausforderungen. Bei ähnlichen Befragungen liegen bei uns jeweils die Sorge um Bürokratie, überbordende Regulierungswut, Fachkräftemangel, Frankenstärke und Herausforderungen mit der Digitalisierung vorne. Aber eben: noch! Denn auch bei uns scheint sich das Klima zu verändern – und zwar nicht zum Guten. Grund genug, das Thema frühzeitig anzupacken und zum Thema des 8. Zentralschweizer Wirtschaftsforums zu machen.



Sicherheit, Verlässlichkeit und Vertrauen als triftige Gründe, in der Schweiz zu investieren: Samih Sawiris im Gespräch mit Moderatorin Susanne Giger

Am Forum wird das Thema aus verschiedenen Optiken angegangen. Einerseits muss der allgemeine Begriff Sicherheit auch ökonomisch beurteilt werden können. Kann man Nutzen und Kosten von Sicherheit bestimmen wie bei anderen Gütern und Dienstleistungen? Es wird bald klar, dass dies schwierig ist und wir stattdessen Grenzkosten und Grenznutzen mehr Beachtung schenken sollten. Doch auch Sicherheit, Verlässlichkeit und Vertrauen als Standortfaktoren müssen genau betrachtet und hinterfragt werden. Insbesondere, wenn eine kleine Minderheit von zehn Prozent sozusagen ein Vetorecht hat und Projekte, Entwicklungen und Ideen behindern oder bereits im Keime ersticken kann. Das grosse Thema am Forum ist schliesslich Cyber

Crime. Metaphorisch angekündigt als das «wachsende und unaufhaltbare Geschwür», scheint sich dies doch zu bewahren. Dies erstaunt kaum, wenn man sich bewusst wird, dass Unternehmen im Durchschnitt erst nach 146 Tagen bemerken, wenn sie einen Virus im System haben. Und dass es im Durchschnitt weitere 32 Tage dauert, um auf das Problem zu reagieren. Da haben wir alle noch ein paar Hausaufgaben vor uns.

Das Programm eines Anlasses wie dem Zentralschweizer Wirtschaftsforum wird geprägt durch seine Referenten. Es ist besonders erfreulich, dass bei der achten Ausführung – neben einer eindrücklichen Palette von 24 hochkarätigen Persönlich-

keiten – zum vierten Mal ein Bundesrat auf dem Pilatus empfangen werden kann. Treffend zur Thematik führt Bundesrat Guy Parmelin durch die vier grossen Bedrohungen für die Schweiz: Terrorismus, Cyber Crime, Naturkatastrophen resp. Pandemien sowie bewaffnete Konflikte, wobei zum letzten Punkt auch der Standpunkt des Bundesrates zu neuen Kampfflugzeugen sowie Boden-Luft-Abwehrsystemen klar dargestellt wird.

Dies alles hat Platz am Zentralschweizer Wirtschaftsforum. Und noch viel mehr! Lesen Sie auf den folgenden Seiten darüber. Wir freuen uns bereits auf das 9. Forum am 4. September 2019!

FH

KOMMENTAR

TOLLE STIMMUNG TROTZ SCHWERVER- DAULICHER KOST

Die Befürchtung, dass die Teilnehmer den Pilatus am Abend des 8. Zentralschweizer Wirtschaftsforums aufgrund des Themas deprimiert und frustriert verlassen würden, traf zum Glück nicht ein. Einmal mehr präsentierte sich der Pilatus von seiner besten Seite: in wunderschöner spätsommerlicher Sonne, in zwar engen, aber passenden Platzverhältnissen, mit einer Infrastruktur, die ihresgleichen sucht auf 2'132 Meter über Meer, verwöhnt von kulinarischen Highlights und freundlichem Personal, konnte das doch eher schwerverdauliche Thema die tolle Stimmung der 240 Teilnehmer nicht trüben. Sichtlich sensibilisiert zum Thema Cyber Security, mit neuen Erkenntnissen zum Gefahrenmanagement, frischen, innovativen Business-Ideen im Bereich Sicherheit und mit vielen Insights zur globalen Bedrohungslage der Schweiz im Rucksack, schauen wir einmal mehr zurück auf ein spannendes, inspirierendes und lehrreiches Zentralschweizer Wirtschaftsforum. Wir haben zugehört, diskutiert, gelernt und schauen nun vorwärts. Wir wollen weiterkommen und Überholtes hinter uns lassen. Wie hat doch der Musicien und Troubadour Bruno Bieri zum Schluss des Anlasses gesagt: «We me wett ga vo A nach B, muess me A la ga.» Wie wahr doch. Wir nehmen es uns zu Herzen!

FH

HOHE ERWARTUNGEN AUF 2'132 M.ü.M



Bei Prachtswetter und in neuer Bestzeit: Das IHZ-Wandergrüppi beim Aufstieg oberhalb der Alp Ämsigen



Das Wirtschaftsforum rollt an: Die Teilnehmer strömen ins Dragon Forum



Einmalige Bergkulisse mit historischer Bausubstanz: Pilatus Kulm als idealer Schauplatz

Das Zentralschweizer Wirtschaftsforum lebt! Dieses wohl wichtigste Get-Together der Wirtschaftsführer der Kantone Luzern, Uri, Schwyz, Ob- und Nidwalden hat sich über die letzten Jahre stetig weiterentwickelt. Damit sind auch die Erwartungen gestiegen und nun an die bereits achte Ausführung dementsprechend hoch. Wie IHZ-Direktor Felix Howald eingangs er-

wähnt, ist es nicht eine Selbstverständlichkeit, die Attraktivität eines solchen Anlasses über viele Jahre aufrechtzuerhalten. Dazu braucht es den Effort vieler Personen und Institutionen, die mitdenken, mitorganisieren und mitfinanzieren. All diesen sei herzlich gedankt! Dank ihnen kann die IHZ auch dieses Jahr die hohen Erwartungen erfüllen.



Die Gastgeber Andreas Ruch und Felix Howald begrüssen die 240 Teilnehmer

Die Teilnehmer erwartet ein spannendes, inspirierendes und abwechslungsreiches Programm zu einem Thema – Sicherheit – welches nicht nur positive Gefühle auslöst. Die intensive Kadenz von Keynotes, Interviews, Workshops und Networking mit insgesamt 25 Referentinnen und Referenten bringen den Teilnehmern viel Hintergrundwissen, neue Insights, überraschende Erkenntnisse und natürlich viele spannende Begegnungen. Denn das Community Building, das Teil-Sein einer Gruppe von Menschen, die ähnliche Herausforderungen teilen und Lösungen entwickeln, ist auch am 8. Zentralschweizer Wirtschaftsforum zentral. Ob Wirtschaftskapitän oder Politikerin, Start-up Unternehmer oder Verwaltungsratspräsidentin, ob jung oder alt, der Austausch ist offen, konstruktiv und lösungsorientiert. Oder wie es ein Neumitglied der IHZ sagt, das zum ersten Mal dabei ist: «Ich hätte nie gedacht, dass ich an nur einem Tag so viele neue spannende Leute kennenlernen und mich mit ihnen austauschen kann.» Für die IHZ heisst dies: Mission accomplished!

FH



Den Nachwuchs fördern – die Zukunft sichern

Von einem Luzerner Stadtbetrieb, gegründet im Jahr 1946, haben wir uns zu einer Unternehmensgruppe mit einem breiten Leistungsspektrum entwickelt. In den Bereichen Elektroinstallationen, integrale Kommunikations- und Sicherheitslösungen, Immobilienentwicklung, Hotellerie, Fassadenbau sowie Maler- und Gipserarbeiten sind wir für Sie ein verlässlicher und professioneller Partner.

Der entscheidende Faktor bei sämtlichen Geschäftsbereichen: sehr gut ausgebildete Mitarbeiterinnen und Mitarbeiter mit ausgeprägten Sozialkompetenzen. Von dieser Überzeugung lassen wir uns leiten, insbesondere bei der Ausbildung unserer 200 Lernenden.

QUALITÄTBEWUSST. NACHHALTIG. INNOVATIV.



Maréchaux-Gruppe

Maréchaux Elektro AG Luzern	BE electric AG Zollikon	Elektro-Kuster AG Engelberg	Widmer Elektro-Telecom AG Ebikon	MVM AG Emmen
Maréchaux Elektro AG Stans	Bonetti Elektro AG Meggen	Elektro QS GmbH Kriens	InfraTech AG Stans	MVM AG Zug
Maréchaux Elektro AG Bern	Cabletron AG Zürich	Elektro Rüegg Cham AG Cham	Radisson Luzern (BHS Hotel AG)	Huwylar Studer AG Luzern
Maréchaux Elektro AG Sursee	Elektro Gotthard AG Andermatt	Hürzeler & Schafroth Elektro-Technik AG Winterthur	Telsec ESS Schweiz AG Wangen	
Maréchaux Electricité SA Lausanne	Elektro Imholz AG Schattdorf	Studer Erwin Elektro AG Römerswil	TurnKey Communication AG Root D4	
Maréchaux Härkingen	Elektro Kaiser AG Sachseln		TurnKey Services AG Root D4	

Maréchaux Elektro AG ◦ Sempacherstrasse 6 ◦ 6003 Luzern ◦ Telefon 041 319 44 44 ◦ Fax 041 319 44 66 ◦ www.marechaux.ch

**EINBRUCHMELDEANLAGEN
ZUTRITTSKONTROLLSYSTEME
VIDEOÜBERWACHUNG**



MASSGESCHNEIDERTE LÖSUNGEN
Sicherheitskonzepte von Telsec ESS



*Wir verkaufen keine Produkte,
sondern Lösungen.*

EINE ÖKONOMISCHE BEURTEILUNG DER SICHERHEIT

Opening Key Note: Überlegungen zum Optimum an Sicherheit und wie politische Institutionen für Sicherheit sorgen.

Professor Reiner Eichenberger wagt sich an die schwierige Aufgabe, das Thema Sicherheit aus ökonomischer Sicht zu beleuchten. Der gemäss kürzlich publiziertem NZZ-Rating zweiteinflussreichste Ökonom der Schweiz weist dabei auf die Bedeutung militärischer, öffentlicher, sozialer, natürlicher und wirtschaftlicher Sicherheit hin. Als grössten Risikofaktor sieht er die Politik.

Reiner Eichenberger geht in seiner Key Note nicht auf die zu bewahrenden Aspekte von Sicherheit ein, weil diese Betrachtung seiner Ansicht nach schlicht langweilig sei. Vielmehr gilt es in Hinblick auf die Zukunft, sinnvolle Rahmenbedingungen zu schaffen, welche Entwicklungschancen für alle ermöglichen – dies ist die entscheidende Sicherheit.

GRENZKOSTEN UND GRENZNUTZEN VON SICHERHEIT

Reiner Eichenberger beginnt mit einem persönlichen Rückblick auf einen seiner ersten Expertenaufträge. Im Rahmen jener Expertentätigkeit ging es darum, Kosten und Nutzen der Schweizer Armee zu evaluieren. In der Ökonomie ist es bekanntlich so, dass im Zusammenspiel zwischen Kosten und Nutzen ein Optimum vermutet werden kann. Die betreffende Studie zu Kosten und Nutzen der Armee war gemäss Reiner Eichenberger allerdings wenig sinnvoll, da sie auf die falsche Frage abzielte. Dass der Nutzen der Armee grösser ist als deren Kosten, war von Anfang an klar. Entscheidend gewesen wäre vielmehr die Frage, ob die Armee mehr nützen oder weniger kosten könnte. Sprich, ob bei gleichem Budget eine höhere Leistung erreicht oder die gleiche Leistung zu tieferen Kosten erreicht werden könnte. Allerdings hatte man auch nach der entsprechenden Studie keinen Anhaltspunkt zu Grenzkosten und Grenznutzen der Armee. Folglich sind die Abwägungen politischer Natur und

es gilt, bildlich gesprochen, zu diskutieren, wie viele Panzer die Schweiz braucht – sind es deren 320, 380 oder gar mehr als 400?

Nach dieser einleitenden Anekdote geht Reiner Eichenberger auf ein zentrales Problem der Schweizer Armee ein: den Mangel an Soldaten. Dieser könnte seiner Ansicht nach leicht behoben werden, indem man gut ausgebildete 26-jährige Soldaten nicht in «Zwangspension» schickt, sondern ihnen stattdessen ein kleines Entgelt bietet für ein paar zusätzliche Wiederholungskurse.

Mit Blick auf die soziale Sicherheit kommt Reiner Eichenberger zur Einsicht, dass das Thema Alterung in den Eidgenössischen Räten als Krankheit behandelt wird. Wir sollten allerdings nicht vergessen, dass wir

«Wir haben einen irren Finanzausgleich! Da lohnt es sich einfach nicht, sich anzustrengen.»

Reiner Eichenberger

älter werden, weil wir gesünder sind. Bezogen auf soziale Sicherheit würde es sich überdies lohnen, darüber nachzudenken, welche Anreize geboten werden müssten, damit Menschen freiwillig über das gesetzliche Rentenalter hinaus weiterarbeiten. Anstelle der heute eher behindernden Rahmenbedingungen könnte man beispielsweise beschliessen, dass arbeitstätige Personen ab 68 Jahren nur noch die Hälfte der Steuern bezahlen müssten. So würden wohl relativ rasch viele Menschen auch nach dem ordentlichen Pensionierungsalter noch freiwillig weiterarbeiten. Insofern bestehen selbst im gegenwärtigen Rentensystem, das Reiner Eichenberger als verrückt bezeichnet, da es auf dem Prinzip beruhe «heute arbeiten

und den Lohn in 20 Jahren erhalten», noch zahlreiche Reformmöglichkeiten.

Doch welches ist der wichtigste Aspekt von Sicherheit? Nach Reiner Eichenberger ist dies ganz eindeutig die Sicherung der Eigentumsrechte. In der Schweiz ist die individuelle Sicherheit sehr gut gelöst. Man stelle sich nur vor, man werde bestohlen oder gar überfallen. Die Täter werden sehr oft dingfest gemacht, auch wenn die Statistiken irrtümlicherweise oft anders interpretiert werden. Die Statistiken zeigen nicht die ganze Wahrheit, da ein einzelner Dieb oder Einbrecher häufig für mehrere Straftaten verantwortlich ist und dies statistisch nur ungenügend berücksichtigt wird. Weiter führt Reiner Eichenberger in seinem Referat aus, dass der Sicherung der Eigentumsrechte des Individuums gegenüber der Gesellschaft ebenfalls sehr grosse Bedeutung zuzumessen ist. Insofern gilt es, staatliche Regulierungen, die den Einzelnen betreffen, sowie das Steuersystem intelligent auszugestalten.

ENTSCHEIDENDE BEDEUTUNG GUTER POLITISCHER INSTITUTIONEN

Um diese Sicherheiten zu erreichen und aufrechtzuerhalten, sind gute politische Institutionen entscheidend. Das beste Militär würde kaum Nutzen stiften, wenn keine funktionierenden politischen Institutionen vorhanden wären – diese sind letztlich ausschlaggebend. Die Schweiz verfügt über gut funktionierende politische Institutionen, da die Politiker hierzulande ein echtes Interesse haben, im Sinne der Bürger zu handeln und das Volkswohl zu maximieren. Als Politiker ist es deshalb auch sachlogisch, sich mit gut organisierten Interessengruppen auseinanderzusetzen, da die Präferenzen der einzelnen Bürger nur schwer abschätzbar sind – zumal die Bürger die eigenen Präferenzen selber oft nicht benennen können. Die funktionierenden politischen Institutionen – insbesondere die direkte Demokratie und das Instrument der Volksinitiative – eignen



Politik als grösstes Sicherheitsrisiko: Professor Reiner Eichenberger mit seiner knallharten ökonomischen Analyse der Politik

sich ausgezeichnet dazu, Minderheiten zu schützen. Insofern hält Reiner Eichenberger auch die seiner Ansicht nach ökonomisch nicht ganz durchdachten Volksinitiativen für nutzbringend. Bürgerinnen und Bürger beschäftigen sich mit interessanten Themen und lernen laufend dazu. Als Anschauungsbeispiele aus der jüngeren Vergangenheit führt er die Vollgeld- oder die Mindestlohninitiative an.

Weitere zentrale Pfeiler der Schweizer Politinstitutionen sind der Föderalismus und die Konkordanz auf den verschiedenen Ebenen. Der Föderalismus wirkt in mehrerer Hinsicht ausgleichend: Er schützt Minderheiten gegenüber Mehrheiten, sorgt für mehr Stabilität über die Generationen und schafft Wettbewerb zwischen den Kantonen. Für künftige Generationen bedeutet Föderalismus mehr Sicherheit, da er ein kurzsichtiges «Schlachten der Milchkühe» verhindert. Gerade im Steuerbereich lässt sich das illustrieren, da Firmen bei

hoher Steuerlast in steuerlich attraktiveren Kantonen abwandern können. Weiter schützt der Föderalismus vor Überschuldung. Auf Gemeinde- und Kantonebene sind es nämlich nicht die zukünftigen, sondern die aktiven Steuerzahler, die die Kosten der Schulden tragen. Wie kürzlich in einer Studie untersucht wurde, schlagen sich Schulden der öffentlichen Hand direkt in den Bodenpreisen nieder, was wiederum für Ausgleichsbewegungen sorgt.

HERAUSFORDERUNGEN UND LÖSUNGSANSÄTZE

Die Eigentumsrechte sind jedoch gemäss Reiner Eichenberger in letzter Zeit in der Schweiz politisch massiv unterwandert worden. Insofern gilt es auch in Zukunft – beispielsweise in Bezug auf den NFA und die Personenfreizügigkeit – intelligente und liberale Anpassungen vorzunehmen, welche die richtigen Anreize setzen.

TB

Lucerne University of Applied Sciences and Arts

HOCHSCHULE LUZERN

Wirtschaft

DER KNOWLEDGE-PARTNER FÜR DIE ZENTRALSCHWEIZ AUCH FÜR IHR UNTERNEHMEN

2017 besuchten rund 1'800 Studierende einen Bachelor- oder Master-Studiengang der Hochschule Luzern – Wirtschaft; über 2'200 Berufsleute absolvierten eine Weiterbildung. In über 129 Forschungs- und Beratungsprojekten unterstützten wir Unternehmen und Institutionen in der Zentralschweiz und in der gesamten Schweiz dabei, komplexe Fragestellungen zu lösen.

Erfahren Sie mehr unter: www.hslu.ch/wirtschaft

Eine der schönsten
Fähigkeiten des Menschen:

Zusammen- stehen.

Wir sehen die Dinge, wie sie für Sie sind. Deshalb helfen wir Ihnen mit unserem betrieblichen Gesundheitsmanagement, die Gesundheit Ihrer Mitarbeitenden zu verbessern und somit Kosten und Absenzen zu vermeiden – damit Ihr Unternehmen gesundheitlich gut dasteht. Gerne beraten wir Sie. **Ganz persönlich.**

Beratung in über 100 Agenturen, per Telefon
unter 058 277 18 00 oder auf css.ch/unternehmen



DIE MIKROPOLE MATTENHOF

EIN SICHERER WERT

Sicher fühlt man sich dann, wenn man seinen nächsten Schritt selber bestimmt. Seine Zukunft selber gestaltet. Genau diese Chance haben Mieter in der Mikropole Mattenhof Luzern. Werden Sie Teil eines neuen Quartiers, prägen Sie es von Anfang an. Und profitieren Sie von der Gewissheit, als Mieter ein interessantes Umfeld vorzufinden. Mieten Sie jetzt hochwertige Büro- und Ladenflächen in flexibler Grösse.

MOBIMO

LUZERNSÜD. STADTEIL MIT ZUKUNFT. info@mattenhofluzern.ch | www.mattenhofluzern.ch

WIE SAMIH SAWIRIS UNSERE SICHERHEIT WAHRNIMMT

Opening Key Note: Gespräch mit Samih Sawiris über den Safe Haven Zentralschweiz: Seine Wertvorstellungen decken sich mit denjenigen der Zentralschweizer.

Samih Sawiris ist seit zehn Jahren in der Zentralschweiz unterwegs. Er hat die Region geprägt wie kaum ein Zweiter. Einige sagen, er habe mit seiner Persönlichkeit gar einen neuen Mindset nach Uri gebracht. Im Gespräch mit der Wirtschaftsredaktorin Susanne Giger spricht Samih Sawiris über seine persönlichen Wertvorstellungen und die Zentralschweiz als Wirtschaftsstandort.

Samih Sawiris passt mit seinem natürlichen, sympathischen, manchmal fast spitzbübischen Lächeln nicht ins Bild des kühl berechnenden Investors. Auf die Einstiegsfrage von Susanne Giger, ob ihm der Vergleich mit Alfred Escher gefalle, wird Sawiris verlegen, zögert erst, und bleibt dann in seiner Antwort bescheiden. Er lobt den Zürcher Alfred Escher als Visionär und erfolgreicher Macher seiner Zeit. Die Welt sei damals auf einer anderen Entwicklungsstufe gewesen, führt der Verwaltungsratspräsident der Orascom Development Holding aus. Die Dinge waren unkomplizierter, die Gesetze und Reglemente noch nicht so umfangreich wie heute. Solch grosse Innovationen wie der Bau der Eisenbahn, die Schaffung der ETH oder die Gründung der Schweizerischen Kreditanstalt (heutige Credit Suisse) seien heute nicht mehr möglich.

DER MENSCH ALS VORBILD

Susanne Giger fasst die Frage zu Alfred Escher etwas weiter und will von Samih Sawiris wissen, ob er denn ein Vorbild in seinem Leben habe. Der Ägypter, der sich an der Technischen Universität Berlin zum Wirtschaftsingenieur ausbilden liess, verneint. Ein eigentliches Vorbild habe er nicht. Vielmehr möchte er als Mensch ein vorbildliches Leben führen. In diesem Sinne kam seinem Patenonkel eine Vorbildfunktion zu. Als Arzt habe dieser menschliche Werte wie Grosszügigkeit, Bescheidenheit und Ehrlichkeit vorgelebt, das habe ihn beeindruckt und beeinflusst. Auch die Zentralschweiz verkörpere diese Werte, was die

Region für ihn besonders attraktiv mache. Er bestätigt, dass die typischen Zentralschweizer Werte weitestgehend deckungsgleich mit seinen persönlichen seien: Bodenständigkeit, Bescheidenheit, Zuverlässigkeit, Offenheit. Er geht sogar noch weiter: Die Zentralschweiz sei im Grunde reicher als die Region Zürich, nur erscheine Zürich oftmals nach aussen reicher. Mit all seinen Charaktereigenschaften versucht der Unternehmer Vorbild zu sein. Gleichzeitig ruft Samih Sawiris dazu auf, mehr Entscheidungen aufgrund des gesunden Menschenverstandes zu treffen, anstatt langwierige Analysen und teure Studien zu erstellen. Er habe damit nur gute Erfahrungen gemacht: Rund 70 Prozent der so gefällten Entscheidungen seien richtig gewesen. Andernfalls wären es vielleicht 80 Prozent gewesen, aber mit unverhältnismässigem Aufwand.

DIE MINDERHEIT IST IN DER SCHWEIZ SEHR ERNST ZU NEHMEN

Susanne Giger spricht den Unternehmer auf sein Projekt in Andermatt an und fragt, wieso die Planung und die Bauarbeiten in Uri so lange gedauert haben. Samih Sawiris, der bereits mit 23 Jahren sein erstes Unternehmen gründete, kommt auf die Rolle der Minderheiten in der Schweiz zu sprechen. Selbst wenn eine Mehrheit der Menschen ein grosses Projekt befürwortet, sei es in der Schweiz praktisch unmöglich, dieses umzusetzen, wenn es von einer Minderheit bekämpft werde. In Andermatt habe er fast fünf Jahre gekämpft, bis eine Baubewilligung ohne Einsprache

«Grosszügigkeit, Bescheidenheit und Ehrlichkeit sind mir wichtig.»

Samih Sawiris



Gekonnt und charmant bringt Moderatorin Susanne Giger neben Sicherheitsaspekten auch persönliche Ansichten aus Investor Samih Sawiris hervor

erteilt wurde. Dank Offenheit, Dialog- und Kompromissbereitschaft habe sich die Minderheit in Andermatt am Ende nicht mehr offen gegen das Projekt gestellt – dies aber erst nach fünf Jahren harter Arbeit! In diesem Sinne sei für ihn die Stärke der Minderheiten vielleicht die grösste Gefahr für die Schweiz. Susanne Giger hakt nach und will wissen, ob er sich mit diesem Wissen noch einmal an das Projekt in Andermatt wagen würde. Samih Sawiris erwidert, dass er sich das im Wissen um dieses Minenfeld wahrscheinlich zweimal überlegen würde.

DIE POLITISCHE STABILITÄT SENKT DIE RISIKORENDITE

Susanne Giger, ehemalige Wirtschaftsredaktorin beim Schweizer Radio und Fernsehen SRF, leitet ihre Frage zur Beurteilung der politischen Stabilität in der Schweiz mit einem Vergleich zwischen Ägypten und der Schweiz ein. Samih Sawiris greift die Gegenüberstellung auf und bestätigt,

dass die wirtschaftliche und politische Stabilität in einem Land einen direkten Einfluss auf die Renditeforderungen von Investoren haben. So sei die Risikoerwartung in Ägypten aufgrund der hohen Unsicherheiten so hoch, dass Investoren für eine Investition bis zu 35 Prozent Rendite fordern. Dank der politischen und wirtschaftlichen Stabilität sei die Risikoerwartung in der Schweiz viel geringer und liege schätzungsweise bei rund vier Prozent. Das sei ein zentraler Vorteil für Investoren in der Schweiz, die diesen hohen Sicherheitsstandard in ihren Erwartungen abbilden.

MAN MERKE SICH, WER VERTRAUEN MISSBRAUCHT

Samih Sawiris war bereits mit 15 Jahren erstmals unternehmerisch tätig, um Geld zu verdienen. Im Gespräch erzählt er, dass sein erstes Handelsgeschäft an der Deutschen Schule in Kairo startete, wo er Lehrern, die nach Deutschland zurückkehrten, Mobiliar abkaufte und dieses auf dem

Markt weiterverkaufte. Vertrauen sei in seiner geschäftlichen Karriere immer zentral gewesen, führt er weiter aus. Auf die Frage von Susanne Geiger, ob sein Vertrauen je missbraucht worden sei, erzählt er nicht ganz ohne Stolz eine kurze Geschichte: Grundsätzlich sollte man über zerbrochenes Vertrauen nicht zu viel nachdenken, denn das beeinflusst einem negativ. Er befolge dabei das Motto: «Thema erledigt – weitergehen!» Allerdings vergesse er Vertrauensbrüche nie! In seiner Jugend habe er einem Kollegen einmal eine elektronische Spielzeuglokomotive verkauft, das Geld dafür habe er aber nie erhalten. Vierzig Jahre später, als sich dieser ehemalige Kollege auf eine Führungsposition bei Orascom beworben hatte, erinnerte sich Samih Sawiris an diesen Vertrauensbruch. Seine Begründung zur Absage der Bewerbung: «Den stellen wir nicht ein, der hat mir einmal eine elektronische Lok geklaut.»

BM

DIGITALISIERUNG UND CYBER SECURITY

Opening Key Note: Digital Warfare – Ist das neue globale Wettrüsten nicht mehr fern oder ist bei unserer Cyber Security alles in bester Ordnung?



Ein Feuerwerk an Argumenten für mehr Cyber Security: Shira Kaplan, Founder & CEO Cyverse AG, bringt viel Know-How und Erfahrung aus dem israelischen Geheimdienst mit in die Zentralschweiz



Hacker, Trojaner, Attacken auf Infrastrukturen – Internet-Kriminalität scheint allgegenwärtig. Wie real sind die digitalen Bedrohungen für Schweizer Unternehmen? Und wie kann man sich dagegen schützen? In ihrer Opening Key Note beantwortet Shira Kaplan wichtige Fragen rund um das Thema Cyber Security.

Schon in IHZ-Direktor Felix Howalds Ankündigung des Referats als «Weckruf für viele unter uns» wird die Brisanz des Themas Cyber Security deutlich. Wieso aber ist der Schutz gegen Angriffe aus dem virtuellen Raum heute so wichtig? Über die letzten Jahre ist die Anzahl der Geräte, die mit dem Internet verbunden sind, rasant gestiegen. Damit, so Shira Kaplan, nimmt auch die Angriffsfläche für Cyber-Attacken zu. Sie verdeutlicht, dass die Anzahl der Wege, über die Angreifer in unsere Unternehmen gelangen können, wachse, wenn Kaffeemaschinen, Snack-Automaten und Kameras in Sitzungszimmern online seien. Gleichzeitig verändert sich der Sicherheitsstatus der Unternehmen aufgrund der fortschreitenden Digitalisierung kontinuierlich. Deshalb liefern auch Sicherheitstests stets nur eine Momentaufnahme. Auch wenn Cyber-Angriffe unterschiedliche Ursachen haben, ist für Shira Kaplan ein Problem offenkundig: Organisationen beweg-

ten sich langsam, Angreifer hingegen seien schnell. Deshalb bietet Shira Kaplan mit ihrem Unternehmen innovative Start-up-Sicherheitskonzepte an. So sei ein Unternehmen in der Lage, ebenso rasch und flexibel zu agieren wie sein Angreifer.

BEDROHUNG AUS DEM DARKNET

Eine sehr beunruhigende Entwicklung stellt das sogenannte Darknet dar. Statistiken zufolge hat die Anzahl der Personen, die über das illegale Netz als Hacker aktiv sind, zwischen 2016 und 2017 um eine Million zugenommen. Es überrascht daher nicht, dass die durch Internet-Kriminalität verursachten Kosten rapide steigen. Entsprechend ist auch die Cyber Security-Branche einer der bedeutendsten Wachstumsmärkte.

«ASSUME BREACH»

Ein wichtiger Ansatz im Umgang mit Cyber Security besteht gemäss Shira Kaplan darin, von einem Angriff auszugehen. «Assume breach» nennt sie diesen Grundsatz. Es geht nicht darum, einen Angriff um jeden Preis zu verhindern, sondern darum, davon auszugehen, dass er bereits vorliegt. Derzeit dauert es im Schnitt 146 Tage, bis ein Unternehmen eine Cyber-Attacke entdeckt, und weitere 32 Tage, bis es darauf reagiert. Mit der «Assume breach»-Perspektive wird der Fokus darauf gelegt, bestehende Angriffe möglichst rasch aufzudecken. So können diese Zeitspannen verkürzt und Schäden verringert werden.

«Organisationen bewegen sich langsam, Angreifer hingegen sind schnell.»

Shira Kaplan

GUTES ZEUGNIS FÜR DIE SCHWEIZ

Trotz der beschriebenen Herausforderungen stellt Kaplan der Schweiz in Sachen Cyber Security ein gutes Zeugnis aus. Dies liegt einerseits daran, dass die Schweiz politisch ein vergleichsweise uninteressantes Ziel darstellt. Andererseits betont Shira Kaplan aber auch die in Schweizer Unternehmen verankerten Grundhaltungen von Zuverlässigkeit und Korrektheit. So würden hierzulande beispielsweise Updates in typisch schweizerischer Zuverlässigkeit regelmässig durchgeführt. Zusammen mit dem allgemein hohen Stellenwert, den die Sicherheit hierzulande genießt, trage vor allem dieser Faktor zur guten Position der Schweiz im internationalen Vergleich bei.

Als Beispiel eines systemkritischen Cyber-Ereignisses in der Schweiz nennt Shira Kaplan Angriffe auf wichtige Infrastrukturen, die sämtliche davon abhängige Unternehmen und Privathaushalte zum Erliegen bringen können. Daneben sieht sie Angriffe auf Core Banking-Systeme und auf die Börsen als die für die Schweiz zentralsten Cyber-Risiken.

Und was wird in der Schweiz als Reaktion auf die steigenden Cyber-Risiken unternommen? Gemäss Shira Kaplan arbeiten Schweizer Unternehmen auf eine zunehmende Automatisierung des Cyber Assessments hin. Gerade grosse Finanzdienstleister hätten festgestellt, dass es nicht genüge, zweimal jährlich eine Risiko-Prüfung vorzunehmen, und setzten daher auf eine ständige automatisierte Überwachung. Daneben beobachtet Shira Kaplan,

dass Unternehmen einen Fokus auf die bessere Sichtbarkeit von Angriffen bis hin zu den Endprodukten legten. Auch die Gefahren des Darknets sind in Schweizer Unternehmen bekannt. Viele Unternehmen überwachen dieses aktiv und nutzen dabei

spezifische Software-Technologien, um zum Beispiel gefälschte Social Media-Seiten zu orten. Und schliesslich geht die Entwicklung in schweizerischen Unternehmen laut Shira Kaplan weg von einer reinen Überwachung der IT hin zu einem umfassenderen Monitoring einschliesslich der OT-Systeme. Für die Zukunft rät sie Unternehmen, vermehrt auch ihre Kooperationspartner ins Cyber-Monitoring einzubeziehen. Denn Angreifer könnten auch über Vertriebspartner oder Lieferanten eindringen.

WENIG CYBER SECURITY-UNTERNEHMEN IN DER SCHWEIZ

Interessanterweise gibt es in der Schweiz trotz des grossen Potenzials nur wenige Start-ups im Bereich Cyber Security. So verzeichnet das Online-Portal start-up.ch in diesem Jahr nur 76 neue Cyber Security-Unternehmen. Im Vergleich dazu wurden in Shira Kaplans Heimat Israel im gleichen Zeitraum über 500 Cyber Security-Firmen gegründet. Diese Start-ups gehen meist auf innovative ehemalige Intelligence- und Cyber Security-Analysten des Militärs zurück, die ihr Know-How nun für zivile Zwecke einsetzen. Auch Shira Kaplans eigenes Unternehmen ist ein solches Beispiel.

Neben den militärischen und politischen Faktoren spielen für die Innovationsstärke Israels im Cyber Security-Bereich auch die Universitäten eine zentrale Rolle. Die Schweiz und ihre Unternehmen müssen sich laut Shira Kaplan folgende wichtigen Fragen stellen: Wer fördert und stärkt die Schweizer Cyber-Industrie? Welche Rolle kann die Armee allenfalls auch hier spielen? Woher kommt das notwendige Kapital? Und wem wollen und können wir vertrauen? Denn gerade im Geschäft mit Cyber Security spielt Vertrauen eine entscheidende Rolle.

IO

CYBER CRIME – EIN TYPISCHER MARKT MIT ANGEBOT UND NACHFRAGE

Zu den Akteuren in einem interessanten Markt und wie sich Unternehmen gegen Cyberangriffe wappnen sollten.

Workshop Cyber Crime

Wir alle sind schon Opfer von Cyber-Kriminalität geworden, selbst wenn wir dies nicht unmittelbar wahrgenommen haben. Insbesondere Unternehmen sind direkt oder indirekt von Cyber-Angriffen betroffen. Zur Vermeidung von Schäden empfiehlt sich deshalb die Umsetzung einiger einfacher Massnahmen.

Als Einstieg in die Diskussion fasst Sita Mazumder die Antworten aller Podiumsteilnehmer auf die Frage zusammen, welche Patzer sie sich im Bereich Cyber Security schon geleistet haben. Matthias Bossardt, Partner bei KPMG, erläutert, wie auf seinem privaten Server Daten wie Hochzeitsfotos und andere Dokumente aufgrund eines Stromunterbruchs und ohne Backup teilweise oder vollständig zerstört wurden. Franz Grüter, Nationalrat und Verwaltungsratspräsident von green.ch, führt aus, dass das Thema Cyber Security in der Pionierphase seines Unternehmens vor rund 15 Jahren noch gar keinen Stellenwert hatte, sondern als Zeichen von Paranoia interpretiert wurde. Das Bewusstsein für dieses wichtige Thema kam erst später auf. Marc Henauer, Chef Schweizerische Melde- und Analysestelle Informationssicherung des Bundes (MELANI), hatte 1984 einen Virus auf dem Computer, was er selber jedoch rund ein Jahr lang nicht bemerkte. Dies wäre heute fatal. Und Armand Portmann, Professor für Cyber Security an der HSLU-Informatik, liess im Jahr 2002 als wissenschaftlicher Mitarbeiter während der Laborbetreuung im Lehrgang MAS Information Security sein Notebook ungesperrt und unbeaufsichtigt zurück – vor den Augen von vielen Berufslernenden, die sich im Thema Cyber Security weiterbildeten. Erfreulicherweise waren die Teilnehmenden des Lehrgangs gnädig und hinterliessen ihm lediglich einen Zettel mit dem Hinweis, doch in Zukunft seinen Computer zu sperren, sobald er den Arbeitsplatz verlässt.

Was waren die ganz grossen Angriffe in letzter Zeit? Marc Henauer zeigt sich erleichtert, dass bei den jüngsten Angriffen keine kritische Infrastruktur direkt betroffen war. Aktuell geht es bei vielen Fällen um Geld und Erpressung. So werden Erpressungstrojaner eingesetzt, welche beispielsweise persönliche Daten verschlüsseln und somit den Eigentümern die Kontrolle darüber entziehen. Will man wieder über die Daten verfügen, muss man ein entsprechendes Lösegeld bezahlen. Teilweise sind auch Sabotagefälle erkennbar, so wurde beispielsweise in der Ukraine zweimal zu Weihnachten, Ende 2015 und Ende 2016, ein Stromausfall provoziert.

WAS IST IN DER VERGANGENHEIT PASSIERT?

Wurde man vor einigen Jahren noch belächelt, wenn man auf das Thema Cyber-Sicherheit hinwies, erhöhte sich das Bewusstsein in der Schweizer Bevölkerung ab 2013 aufgrund der öffentlich bekannt gewordenen Fälle signifikant. Beispielsweise wurde die PostFinance für zwei Tage blockiert, weil das Finanzinstitut

Julian Assanges Kreditkarte deaktiviert. Weitere bekannte Fälle sind Interdiscount, Digitec oder RUAG. Letzterer ist insofern bemerkenswert, als dass die RUAG während 18 Monaten nicht bemerkte, dass ein Angriff stattfindet. Zudem hat man auch nach zweijähriger Untersuchung nicht herausgefunden, wer für den Angriff verantwortlich war. Dies sind jedoch lediglich die prominentesten Fälle, die Dunkelziffer dürfte sehr hoch sein.

WIE HAT SICH DAS BEWUSSTSEIN ENTWICKELT?

Armand Portmann führte an der Hochschule Luzern im Jahr 2016 eine Studie zu Cyber-Angriffen durch, die ergab, dass mehr als die Hälfte der teilnehmenden Firmen in irgendeiner Form schon von Vorfällen im Bereich Cybersicherheit betroffen war und mehr als 15 Prozent als Folge davon Betriebsstörungen zu verzeichnen hatte. Das Unternehmen KPMG führt regelmässige Erhebungen zur Betroffenheit durch. Letztes Jahr sagten 88 Prozent, sie seien negativ betroffen gewesen. Diese Zahlen sind zwar mit viel Unsicherheit behaftet. Der springende Punkt ist allerdings nicht, ob es einem getroffen hat oder nicht. Vielmehr geht es um die Erkenntnis, dass man aktiv werden muss. Ein wichtiger Punkt der diesjährigen KPMG-Studie ist die teilweise zu beobachtende Inkonsistenz: auch wenn in Verwaltungsräten in den letzten drei bis vier Jahren viel über Cyber-Kriminalität gesprochen und grundsätzlicher Handlungsbedarf festgestellt wurde, gibt es immer noch Leute, die nicht an eine direkte Betroffenheit glauben und sich erst bewegen wollen, wenn Cyber Crime-Vorfälle in einem Unternehmen in der gleichen Branche in der gleichen Region registriert wurden. Dieser Ansatz dürfte sich jedoch als gefährlich fahrlässig herausstellen.

Warum Cyber-Attacken? Und wie sieht der entsprechende Markt aus? Franz Grüter sieht in Cyber-Attacken ein neues Phänomen, nach welchem sich eben nicht nur kriminelle Einzelakteure, sondern zunehmend auch Staaten im Cyber-Raum neue Machteinflussbereiche erschliessen. Man sehe sich nur einmal das jährliche Budget der NSA an – dieses beträgt 10 Mia. US-Dollar, was dem Doppelten des gesamten Schweizer Rüstungsbudgets entspricht. Die NSA beschäftigt rund 6'500 Vollzeitangestellte und greift auf die Dienste von mehreren zehntausend externen Personen zurück. Zudem ist die NSA nicht nur defensiv, sondern auch offensiv tätig. Dies trifft ebenso auf die Nationen Indien und China zu. Im kürzlich

WARUM CYBER-ATTACKEN? UND WIE SIEHT DER ENTSPRECHENDE MARKT AUS?

publizierten Fünfjahresbericht der NSA steht, was die Organisation alles auf dem Radar habe. Es geht mitunter um die Möglichkeit, offensiv ein System lahmzulegen oder zu beeinflussen – wie beispielsweise ein E-Voting System.



Sita Mazumder, Dozentin an der Hochschule Luzern, moderiert mit Sachwissen und Erfahrung den Workshop zu Cyber Crime

Die staatliche Dimension ist nur die eine Seite. Es gibt noch weitere aktive Mitspieler. Wenn man an kriminelle Organisationen denkt, könnte man auf die Idee kommen, es laufe ähnlich wie im Spielfilm «Der Pate» ab. Dem ist jedoch nicht so. Es handelt sich um einen hochspezialisierten und rational arbeitsteiligen Markt. Marc Henauer berichtet, wie man sich in der Vorgängerorganisation der MELANI einmal die Mühe gemacht habe, eine Karte des kriminellen Untergrunds anzufertigen. Schliesslich ist man auf eine Karte mit rund 2'500 Punkten gekommen, die dem schematisch dargestellten Luftverkehr über Europa zu Stosszeiten gleicht. Es gibt sehr viele Leute, die ausserordentlich gut sind auf einem ganz bestimmten Gebiet. Beispielsweise gibt es

Den Angreifern geht es nicht nur um Geld, sondern auch um Intellectual Property. Den staatlichen Akteuren geht es um Macht. Diese Motivationen liegen aber gar nicht allzu weit voneinander entfernt. Schon in der Vergangenheit war zu beobachten, dass die Instrumente für Angriffe von staatlichen Akteuren entwickelt wurden und dann unbeabsichtigt an die Öffentlichkeit gelangten.

In gewissen Ländern sind kriminelle Machenschaften nicht nur via Darknet, sondern gar über ganz normale Webseiten käuflich – in Russland gibt es Webseiten, auf denen man bereits ab zehn US-Dollar sogenannte DDoS-Attacken kaufen kann, um beispielsweise gezielt Webseiten lahmzulegen. Insofern wird mittlerweile auch von «Crime-as-a-Service» gesprochen. Es gibt viele Personen, die technisch sehr versiert sind und ihre Dienste über Plattformen anbieten. Beispielsweise werden gehackte Computer oder geklaute Daten feilgeboten.



Nationalrat und IT-Unternehmer Franz Grüter weist auf das vielschichtige Bedrohungspotenzial von Datenmissbrauch hin – nicht nur beim E-Voting

Personen, die sich auf das Programmieren spezialisiert haben und andere, die bestens Bescheid wissen, wie man mit Webseiten umgeht. Es handelt sich um einen ganz normalen Markt mit Angebot und Nachfrage. Das Bild eines pubertierenden Computer-Nerds im Teenageralter, der zurückgezogen im Keller der Grossmutter lebt, ist ein unzutreffendes Klischee. Es sind Leute aktiv, die «extrem gute Geschäftsideen» haben. Sie heuern entsprechende Spezialisten an, die quasi im Auftragsverhältnis das Produkt entwickeln und umsetzen. In diesem Markt gibt es keine Arbeitsgesetze, keine Arbeitsgerichte, keine Gewerkschaften und dergleichen. Die Unternehmen agieren dynamisch und funktionieren ganz wie KMUs, beispielsweise um Ransomware zu verteilen oder Spitaler zu erpressen. Diese informellen Unternehmen funktionieren so lange, wie es Renditen zu holen gibt. Wer steckt also hinter den kriminellen Machenschaften? Vereinfacht gesagt sind es dynamische, motivierte und überaus spezialisierte Unternehmertypen! Die Innovation in diesem Markt ist bemerkenswert.

WIE SOLLEN SICH UNTERNEHMEN VERHALTEN?

Ein erstes Handlungsfeld zeigt sich auf der Bildungsseite. Es ist bekannt, dass gute Sicherheitsbeauftragte Mangelware sind. Dennoch gibt es zielführende Weiterbildungsangebote auf tertiärer Stufe. Neuerdings gibt es gar Bachelor-Studiengänge, die sich primär um das Themenfeld Cyber and Information Security drehen. Aber auch der Staat ist gefordert und hat die Aufgabe, seine eigene kritische Infrastruktur zu schützen.

Darüber hinaus muss er Angriffe innert nützlicher Frist erkennen und sich ein Bild der Lage machen können. Dies mitunter auch, um die Wirtschaft zu informieren. Insofern sind diverse Bestrebungen im Gange. So wird die Armee beispielsweise eine Cyber-RS aufgleisen. Trotzdem bleibt zu kritisieren, dass die Schweiz zwar seit nunmehr sechs Jahren eine nationale Cyber-Strategie hat, man sich beim Bund allerdings immer noch uneinig ist, wer dafür zuständig ist.

DIE REFERENTEN DES WORKSHOPS

- Matthias Bossardt, Partner, Head of Cyber Security, KPMG
- Franz Grüter, VRP green.ch und Nationalrat Luzern
- Marc Henauer, Chef Schweizerische Melde- und Analysestelle Informationssicherung des Bundes (MELANI)
- Armand Portmann, Dozent Hochschule Luzern - Informatik
- Moderation: Sita Mazumder, Dozentin Hochschule Luzern - Informatik

Doch wo sollen Unternehmen am besten ansetzen? Einerseits ist zu empfehlen, dass das Thema Cyber Security in den Verantwortungsbereich des Managements gehört und in das Risikomanagement eines Unternehmens integriert werden sollte. Es kann insofern nicht die Aufgabe eines einzelnen IT-Mitarbeitenden sein, die ganze Cyber Security für ein Unternehmen zu verantworten. Andererseits ist es wichtig, einige zentrale Massnahmen prioritär anzugehen. Zwar wurde kürzlich vom Bundesamt für Wirtschaftliche Landesversorgung ein Minimalstandard mit 160 Massnahmen veröffentlicht. Das ist jedoch nicht wirklich nützlich für KMUs, die Prioritäten setzen müssen. Matthias Bossardt empfiehlt die Umsetzung von zwölf elementaren Massnahmen. So soll klar definiert werden, wer sich um was kümmert und wer was koordiniert. Weiter sollen Unternehmen festhalten, was es überhaupt zu schützen gilt – was sind die «Kronjuwelen»? Es muss genauestens verstanden werden, was ein angreifendes Unternehmen errei-

chen will. Weiter gilt es Ordnung zu schaffen und zu analysieren, wie die IT-Struktur aussieht. Hier muss auch die sogenannte «Shadow IT» mitberücksichtigt werden, was bedeutet, dass man unter anderem Klarheit darüber haben sollte, wie viele und welche Clouddienste verwendet werden. Oft sind das signifikant mehr als man vermutet. Weitere Massnahmen sind die Schulung und Sensibilisierung von Mitarbeitenden, das Beschränken von Zugriffen und Machtballungen, das regelmässige oder automatische Aktualisieren der Systeme, die laufende Überprüfung auf Malware, die laufende Überwachung der Netzwerke, das Vornehmen von Datensicherungen und technische Überprüfungen. Darüber hinaus empfiehlt es sich, beim Erschliessen neuer Geschäftsfelder konsequent an die Sicherheit und den Datenschutz zu denken. Als letzten Punkt nennt Matthias Bossardt das regelmässige Testen der Systeme. Die Summe dieser Massnahmen kostet nicht viel und kann dennoch einen grossen Teil der potenziellen Vorfälle verhindern.



Die Panelisten sind sich einig: Der Cyber Security-Schnelltest für KMU ist ein gutes Instrument, um Unternehmen vor Angriffen aus dem Cyberspace zu schützen und darauf vorzubereiten

DIE RISIKOBEURTEILUNG GEHÖRT INS PFLICHTENHEFT JEDER GESCHÄFTSLEITUNG

Sicherheit hat nicht nur einen Preis, sondern auch einen Wert. Die grössten Gefahren für Unternehmen – und was wir dagegen tun können.

Workshop Gefahren-Management

Die Beurteilung von Klein- und Grossrisiken wird von Unternehmen oft vernachlässigt. Dabei können ein geschärftes Risikobewusstsein und eine gute Risikobeurteilung gerade im Krisenfall entscheidende Erfolgsfaktoren sein. Die Experten sind sich einig: Das klassische Risikomanagement gehört ins Pflichtenheft jeder Geschäftsleitung.

Moderator Christoph Lengwiler eliminiert gleich zu Beginn seiner Einführung vorbildhaft eine erste Gefahrenquelle: Er schaltet das Risiko einer potenziellen Zeitüberschreitung aus, indem er einen Wecker stellt. Anschliessend stellt er die Runde vor, beginnend bei Jürg Wobmann, Kommandant der Kantonspolizei Nidwalden und designerter Chef der Luzerner Kriminalpolizei. In seiner Rolle als Polizeikommandant vertritt Jürg Wobmann vor allem die Sicht der Blaulichtorganisationen und erläutert die Zusammenarbeit zwischen den verschiedenen Organisationen im Ereignisfall. Benno Bühlmann, Direktor beim Bundesamt für Bevölkerungsschutz BABS und in dieser Funktion auch Mitglied der Departementsleitung des Eidgenössischen Departments für Verteidigung, Bevölkerungsschutz und Sport VBS, erklärt in dieser Diskussionsrunde die Aufgaben des Bundes im Katastrophenschutz und Krisenfall. Philipp Gmür, Group CEO bei der Helvetia, bringt die Sicht der Versicherungsbranche ein und erläutert, welche Risiken versichert werden können, und welche nicht. Und schliesslich Beat Hodel, Mitglied der Geschäftsleitung und Leiter Krisenstab bei der Luzerner Kantonalbank (LUKB), der auf die operative Umsetzung von Katastrophenplanungen bei Unternehmen eingeht.

«In der Risikobeurteilung gibt es keine universell gültigen Empfehlungen.»

Beat Hodel

der Kantonbank in Emmenbrücke vor Überschwemmungen gesichert.

Philipp Gmür führt ebenfalls das Hochwasser 2005 als ein bleibendes Ereignis in seiner Karriere aus. Obschon er berufsbedingt mit vielen prägenden Schadensfällen konfrontiert ist, ragt dieses Unwetter heraus. Er kann sich erinnern, wie die Banken versucht haben, nasse Banknoten zu trocknen. Dabei stellte sich insbesondere für sie als Versicherer die Frage, wer für welche Schäden aufkommen müsse. Ferner erinnert sich Philipp Gmür an das Hochwasser in Brig 1993, als die Versicherungsbranche praktisch einen neuen Stadtkern finanzierte. In Erinnerung geblieben ist ihm auch ein Fall vor etwas mehr als zehn Jahren, als ein Mitarbeiter ungewollt einen Computer-Virus in das System einschleuste. Das war ein Ereignis, auf welches die Versicherungsindustrie damals noch wenig sensibilisiert war, heute ist das anders.

Jürg Wobmann hat ebenso bleibende Erinnerungen an das Jahrhundert-Hochwasser. Einprägsam waren für ihn insbesondere die räumlichen und zeitlichen Dimensionen des Ereignisses, das sämtliche Organisationen vor Herausforderungen neuen Ausmasses stellte. Eindringlich war für ihn die Erkenntnis, dass Buochs vom Hochwasser praktisch verschont



Orten Handlungsbedarf sowohl bei den Unternehmen wie bei der öffentlichen Hand: Die Panelisten des Workshops Gefahren-Management

DAS JAHRHUNDERT-HOCHWASSER 2005 BLEIBT IN ERINNERUNG

Christoph Lengwiler startet die Runde mit der Frage, welches das prägendste oder gravierendste Schadensereignis in den beruflichen Karrieren der erfahrenen Diskussionssteilnehmer war. Beat Hodel beantwortet die Frage ohne zu zögern mit dem Jahrhundert-Hochwasser im Jahr 2005, das die Zentralschweiz besonders hart getroffen hatte. Er beschreibt, wie die LUKB damals mehrere Tage im Krisenmodus operierte. Den Regionalsitz in Emmenbrücke hatte die Bank aufgrund der Überschwemmung verloren, die gesamte Filiale sei unter Wasser gestanden. Der Tresorraum sowie darin verwahrte Gegenstände seien massiv beschädigt worden, der Betrieb musste vollständig eingestellt werden. Parallel dazu drohte auch der Hauptsitz in Luzern durch die Reuss überschwemmt zu werden. Beat Hodel hält fest, dass im Nachgang zu diesem Hochwasser grosse Investitionen im Bereich Hochwasserschutz getätigt wurden. So ist beispielsweise der heutige Tre-

«Sicherheit hat einen Preis, aber auch einen Wert.»

Benno Bühlmann

mediale Aufmerksamkeit das tragische Ereignis weiter auf.

Benno Bühlmann schliesst sich seinen Diskussionspartnern an. Im Jahr 2005 war er Leiter des Amtes für Umweltschutz in Uri und hatte das Hochwasser entsprechend hautnah miterlebt. Er habe in einer einzigen Woche fünf Kilo abgenommen. Dann bleibt ihm aber auch der Brand im Gottardtunnel 2001 mit elf Toten und vielen Verletzten in Erinnerung. Die emotionale



Dozent Christoph Lengwiler von der Hochschule Luzern zeigt vollen Einsatz, um mit seinem Sales Pitch weitere Teilnehmer in seinen Workshop zu locken

Belastung war gross, die Bewältigung des weltweiten Medieninteresses vor Ort herausfordernd.

GROSSRISIKEN WERDEN VOM BUND BEARBEITET

Christoph Lengwiler fragt in die Runde, wie die Aufgabenteilung zwischen den Institutionen bei Grossrisiken aussehe. Benno Bühlmann erklärt, Grossrisiken würden grundsätzlich vom Bund bearbeitet. Hier stelle sich die Frage, was denn überhaupt mögliche Risiken seien und welches Schadenspotenzial diesen attestiert würden. Dazu hat das BABS Szenarien zu Gefährdungen der Schweiz erarbeitet. Diese sind auf www.babs.admin.ch ersichtlich. Demnach lauten die Top-3 Ereignisse nach finanziellem Schadenspotenzial wie folgt: 1) Erdbeben, 2) Strommangel, 3) Pandemie. Der Bund sensibilisiere die nationalen Blaulichtorganisationen, um Vorkehrung auf diese Gefahren treffen zu können. Benno Bühlmann appelliert aber

eingetroffen ist, heisst das nicht, dass es nicht trotzdem geschehen kann. Oder: Was nicht sein darf, kann auch nicht sein! Heute versichert man nur Risiken, die man effektiv kennt, beispielsweise Autos, Häuser, Liegenschaften. Aber weitere grosse Risiken werden heute nicht versichert, obschon die Verletzlichkeit und das Schadenspotenzial – unter anderem durch die zunehmende Vernetzung – exponentiell zugenommen haben. Philipp Gmür erklärt, man habe in den vergangenen Jahren das Risikobewusstsein verloren. Dafür spricht auch, und da widerspricht Philipp Gmür teilweise Benno Bühlmann, dass die Bevölkerung die Top-3 Risiken, die der Bund identifiziert hat, grossmehrfach nicht kennt oder berücksichtigt. Die Bevölkerung ist zu wenig darauf sensibilisiert. Benno Bühlmann entgegnet, dass die Probleme eben auch finanzieller Natur seien. Um im Krisenfall bereit zu sein, müsste man Mittel zur Verfügung stellen wie beispielsweise Spitalbetten. Doch aus finanziellen Gründen werden diese Vorkehrungen oftmals nicht getroffen.

RISIKOBEURTEILUNG IST EINE GESCHÄFTSLEITUNGSPFLICHT

Benno Bühlmann appelliert an die Zuhörer, dass jedes Unternehmen eine risikobasierte Gefahrenanalyse durchführen sollte. Dazu gibt es Leitfäden, um relevante Risiken zu erkennen und zu identifizieren. Auf dieser Basis kann die Geschäftsleitung entscheiden, welche Massnahmen man zur Risiko- oder Schadenspotenzialreduktion ergreifen will. Oftmals bewirken schon kleine Vorkehrungen eine potenziell hohe Schadensminimierungsquote. Eine solche Risikobeurteilung gehöre zum Pflichtenheft jedes Unternehmens und liege in der Verantwortung der Geschäftsleitung. Jürg Wobmann ergänzt, dass dazu auch Szenarienpläne für andere mögliche unternehmensrelevante Ereignisse gehörten wie z.B. Drohungen, Erpressungen, Todesfälle, Androhung eines Amoklaufs. Hier empfehle sich das Erstellen von sogenannten Verhaltensempfehlungen oder Einsatzregeln (Rules of Engagement). Jürg Wobmann bestätigt, dass Unternehmen bei ihnen nicht selten nach Hilfe beim Erstellen von Notfallkonzepten fragen. Beat Hodel ergänzt, dass jede Ri-

«Wir müssen unser Risikobewusstsein wieder stärken.»

Philipp Gmür

Dieser Bewertung sollten wir mehr Beachtung schenken, ist Benno Bühlmann überzeugt und ruft alle im Raum auf: Dran bleiben bei der kontinuierlichen Risikoanalyse! Jürg Wobmann schliesslich schlägt an dieser Stelle den Bogen zur Key Note von Professor Reiner Eichenberger. Er betont den ökonomischen Nutzen, wonach Sicherheit auch ein bedeutender Standortvorteil ist. Und schliesslich kommt er auf die Schlussfrage von Christoph Lengwiler zurück und stellt die Gegenfrage: «Wo ist es denn sicherer als hier in Zentralschweiz?»

DIE REFERENTEN DES WORKSHOPS

- Benno Bühlmann, Direktor Bundesamt für Bevölkerungsschutz
- Philipp Gmür, Group CEO Helvetia Versicherungen
- Beat Hodel, Mitglied GL und Leiter Krisenstab Luzerner Kantonalbank AG
- Jürg Wobmann, Kommandant Kantonspolizei Nidwalden
- Moderation: Christoph Lengwiler, Dozent Hochschule Luzern - Wirtschaft

WIR KÖNNEN UNS SICHER FÜHLEN

Als Abschluss der angeregten Diskussionsrunde stellt Christoph Lengwiler die Frage in den Raum, ob wir uns in der Zentralschweiz sicher fühlen können. Beat Hodel nimmt den Ball von Christoph Lengwiler auf und betont, dass wir sicherlich noch mehr machen könnten. Wichtig sei – und da appelliert er direkt an die Zuhörer – dass jeder Einzelne für seine Risiken vorbeugen müsse. Sicherheit ist immer auch Selbstverantwortung. Darüberhinaus betont er nochmals, dass die stetige Zusammenarbeit zwischen sämtlichen involvierten Organisationen und die Vorbereitung auf mögliche Ereignisse wichtig seien, um im Ereignisfall schnell und effizient handeln zu können. Philipp Gmür pflichtet seinem Vorredner bei. Wichtig sei auch, das Risikobewusstsein zu stärken. Oftmals reichen schon kleine Vorkehrungen aus, um grosse Schäden abzuwenden. Benno Bühlmann fordert nochmals, auch einmal das Udenkbare zu denken. Sicherheit habe nicht nur einen Preis, sondern eben auch einen Wert.



Das rege Interesse zeigt klar, dass Gefahren-Management für Zentralschweizer Unternehmen kein Fremdwort ist

**Die starke Partnerin der
Zentralschweizer KMU.**

Erfolg ist individuell. Lassen Sie sich deshalb massgeschneidert und persönlich beraten.

www.kantonalbank.ch

Gemeinsam wachsen.  **Kantonalbank**

Nichts zu tun ist keine Option

Ein solider Schutz gegen Cyberangriffe ist in unserer daten- und technologiebasierten Wirtschaft entscheidend. Cybersicherheit sollte deshalb im Mittelpunkt jeder nachhaltigen Wachstumsstrategie stehen. Doch welche Massnahmen gilt es zu ergreifen? KPMG hilft Ihnen, mit technischer Expertise und digitaler Innovationskraft, Risiken zu reduzieren und Vertrauen zu fördern.

Anticipate tomorrow. Deliver today.

Kontakt

Thomas Affolter, Leiter Marktregion Zentralschweiz
+41 58 249 49 82, taffolter@kpmg.com, kpmg.ch

KPMG



DIE (ZENTRAL)SCHWEIZ SICHERER MACHEN – WIE GEHT DAS?

Die Schweiz ist der ideale Standort für das Sicherheitsgeschäft.

Workshop Sicherheit als Geschäftsfeld

Armee, Sicherheitsdienste, Sicherheitsdruck, Fälschungsschutz: Die wachsende Sorge um Sicherheit hat eine Vielzahl von Unternehmen hervorgebracht, die die Welt sicherer machen wollen. Im Workshop «Sicherheit als Geschäftsfeld» diskutieren Branchenvertreter ihren Markt, dessen Zukunft, den Standort Schweiz und die Frage, wie man Sicherheit verkaufen kann.

Alle Podiumsteilnehmer vertreten Unternehmen oder Organisationen, die sich zum Ziel gesetzt haben, die Welt sicherer zu machen. Wie wollen sie das konkret erreichen? Und was verstehen Unternehmensvertreter, die sich tagtäglich mit der Thematik befassen, überhaupt unter Sicherheit? Rüstungschef Martin Sonderegger erläutert, die primäre Rolle der armasuisse bestehe darin, die nötigen Technologien, Materialien und Güter zu beschaffen, damit die Armee ihre Aufgaben im Bereich Sicherheit erfüllen könne. Beat Glutz von Blotzheim, Geschäftsleitungsvorsitzender der Securitas AG, bezeichnet die Securitas als Synonym für private Sicherheitsdienste in der Schweiz. Sicherheit verstehe er als Schutz vor Gefahren. Er unterscheidet dabei zwei Arten von Gefahren: Aktive Gefahren, die von Menschen oder Gruppen ausgehen, die etwas Schädliches tun oder bezwecken. Den Schutz gegen solche Gefahren bezeichnet er als «Security». Vor den passiven Gefahren wie beispielsweise Unwetterrisiken schütze man sich demgegenüber mit sogenannten «Safety»-Massnahmen. Das Geschäftsmodell der Securitas bestehe im Verkauf von Dienstleistungen in beiden Bereichen.

In einem anderen Feld des Sicherheitsmarktes ist die Hunkeler AG Paper Processing tätig, die unter anderem auf Digitaldrucksysteme für die Verarbeitung sicherheitsrelevanter Dokumente spezialisiert ist. Auch die Firma DPS AG hat sich dem Sicherheitsaspekt des Fälschungsschutzes verschrieben. Sie bietet insbesondere magnetische, unsichtbare, bio-verschlüsselte Sicherheitslösungen an. Sowohl für Hans Gut, Geschäftsleitungsmitglied der Hunkeler AG, als auch für Thomas Villwock, CEO der DPS AG, stehen in ihrem Geschäft jeweils innovative Technologien im Zentrum, die dazu genutzt werden, die Sicherheit in verschiedenen, für den Kunden zentralen, Bereichen zu gewähren oder zu erhöhen.

PRIVATE GEWINNEN AN BEDEUTUNG

Eine Besonderheit der Sicherheitsbranche ist ihre Nähe sowie teilweise Überschneidung mit staatlichen Sicherheitsaufgaben. So ist etwa die Securitas neben dem privaten Sicherheitsdienst auch stark im Bereich der öffentlichen Sicherheit tätig und wird in dieser Funktion von der Bevölkerung wahrgenommen und akzeptiert. Laut Beat Glutz von Blotzheim verzeichnet die Securitas gerade bei der Übernahme von öffentlichen Aufgaben wie Gefangenentransporten oder Hilfspolizeidiensten ein starkes Wachstum. Obwohl dies für die Geschäftsentwicklung positiv ist, gebe es seines Erachtens zu wenig Vorschriften in diesem sensiblen Bereich, etwa hinsichtlich der Bedingungen, die eine Person erfüllen müsse, um als Mitarbeiter eines privaten Sicherheitsunternehmens öffentliche Aufgaben wahrnehmen zu dürfen. Die Securitas verfüge zwar über interne

Regularien, leide aber unter den allgemein tiefen Eintrittshürden, die zum Einstieg in den boomenden Markt einladen. Deshalb setze sich die Securitas zum Schutz des Rufes der Branche für eine aktive Regulierung ein.

Die Nähe zwischen öffentlicher und privater Sicherheit wird auch von Martin Sonderegger unterstrichen. In den letzten Jahren sei eine vermehrte Auslagerung von öffentlichen Aufgaben im Sicherheitsbereich an Private zu beobachten. Dies ist laut Martin Sonderegger vor allem auf den Finanzdruck und damit einhergehende Stellenreduktionen zurückzuführen, die den Staat dazu zwingen, sich auch im Bereich Sicherheit auf die Kerntätigkeiten zu konzentrieren und Aufgaben wie beispielsweise Logendienste von privaten Anbietern abdecken zu lassen.

«In Zukunft geht es darum, den optimalen Mix zwischen Technik und Mensch zu finden.»

Beat Glutz von Blotzheim

DIE ZUKUNFT DES SICHERHEITSMARKTES

Gefragt nach neuen Geschäftsfeldern im Sicherheitsmarkt der Zukunft, sieht Thomas Villwock im eigenen Geschäftsbereich der DPS AG, der Verhinderung von Fälschungen, ein enormes Potenzial. Er erklärt, dass sich viele Produzenten von Markenprodukten, sei es in der Luxusgüterbranche oder in der Pharmaindustrie, mit der Situation konfrontiert sehen, dass über 50 Prozent der sich im Umlauf befindenden Produktion gefälscht sei. Dadurch wird das Wertempfinden ausgehöhlt und den Originalproduzenten fehlen die Mittel, um weiterhin in innovative Produkte zu investieren. «Das ist eine Art Krebs, der bekämpft werden muss», schliesst Thomas Villwock sein Votum bildlich.

Auch Hans Gut attestiert dem Geschäftsbereich, in welchem er mit der Hunkeler AG aktiv ist, besonders gute Zukunftsaussichten. Zwar wird oft gesagt, die Druckindustrie stehe vor dem Aus und tatsächlich markierte die Digitalisierung für die Branche einen Paradigmenwechsel. Doch ist das Potenzial beispielsweise bei der on demand-Produktion von Büchern oder im Verpackungsdruck laut Hans Gut gewaltig, vor allem, wenn es darum geht, mittels Drucktechnologien die Verfolgung von Produkten durch die gesamte Logistikkette zu ermöglichen.

Beat Glutz von Blotzheim von der Securitas sieht mit Blick auf das Geschäftsfeld der Sicherheitsdienstleistungen zwei zukünftige Stossrichtungen. Einerseits gehe es, etwa im Bereich von Überwachungsleistungen, darum, den optimalen Mix zwischen Technik und Mensch zu finden. Andererseits müsse die Digitalisierung gezielt genutzt werden. Hier bieten sich Chancen, die Kundschaft enger mit den Securitas-Mitarbeitenden zu verbinden. So werde Vertrauen geschaffen, indem der Kunde etwa das Personenprofil des beauftragten Securitas-Mitarbeitenden einsehen und online dessen Aktivitäten nachverfolgen könne. Daneben unter-



Wirbt mit Worten, Namen und Inhalt: HSLU-Dozent Christoph Hauser bei der Vorstellung seines Workshops

stützt die Digitalisierung auch erweiterte Möglichkeiten im Bereich von kurzfristigen on demand-Services (z.B. Entgegennahme von Lieferungen).

CYBER SECURITY VERÄNDERT AUCH DAS RÜSTUNGSGESCHÄFT

Aus dem Publikum wird die Frage an Martin Sonderegger gestellt, ob er durch die zunehmende Bedeutung der Cyber Security eine Veränderung in seiner Tätigkeit spüre. Hierauf führt der Rüstungschef aus, dass eine klare Verlagerung in den IT-Bereich erfolge. «Ein neues Kampfflugzeug ist nicht mehr primär ein Flugzeug, sondern – etwas überspitzt formuliert – ein Computer, der nebenbei noch fliegen kann.» Dasselbe gelte auch im Telekommunikationsbereich, wo nicht mehr klassische Funkgeräte, sondern vielmehr digitale Netzwerkstrukturen genutzt werden. Angesichts dieser Entwicklungen wird die Qualitätsevaluation bei der Beschaffung immer komplexer. Deshalb ist es laut Martin Sonderegger zentral, dass die armasuisse über hochqualifizierte Mitarbeiter verfüge, die umfassende eigene Material-

hat, insbesondere für die Securitas. Als Beispiele nennt er die Übernahme von Diensten der Alarmzentralen für Aufzüge oder die Durchführung von präventiven Kontrollen an Grossveranstaltungen. Und so beobachtet Beat Glutz von Blotzheim in der Schweiz auch, dass die «Safety»-Ansprüche viel grösser sind als die «Security»-Bedürfnisse. Seiner Meinung nach trägt gerade dies dazu bei, dass die Schweiz von aussen als sicher wahrgenommen wird.

WIE VERKAUFT MAN SICHERHEIT?

Um den geschäftlichen Aspekt anzusprechen, richtet Moderator Christoph Hauser seine Frage bewusst etwas provokativ an die Podiumsteilnehmer: «Wie verkauft man Sicherheit – etwas, das man im besten Fall, wenn alles gut läuft, gar nicht spürt? Machen Sie den Leuten Angst?» Thomas Villwock führt dazu aus, im Fall der DPS AG sei es viel eher so, dass es die Kunden waren, die ihm Angst gemacht hatten, als sie über das Ausmass der Fälschungsaktivitäten berichteten. Ein Bedürfnis sei hier also an ihn herangetragen worden und sein Unternehmen habe in der Folge eine

DIE REFERENTEN DES WORKSHOPS

- Beat Glutz von Blotzheim, Vorsitzender der Geschäftsleitung Securitas AG
- Hans Gut, Mitglied GL und Leiter Marketing/Strategisches Partnering Hunkeler AG Paper Processing
- Martin Sonderegger, Rüstungschef armasuisse
- Thomas Villwock, CEO DPS AG
- Moderation: Christoph Hauser, Dozent Hochschule Luzern - Wirtschaft

von Kundenseite an das Unternehmen herangetragen wurden. Allerdings sei der Markt in den letzten Jahren härter geworden und man könne sich nicht mehr auf eine ausschliesslich reaktive Rolle beschränken. Stattdessen müsse man sich vermehrt in die Lage der Kunden hineinversetzen und sich fragen, wo Sicherheitsbedürfnisse bestehen. Sind diese noch nicht abgedeckt, sieht es die Securitas als ihre Aufgabe, dem Kunden eine Lösung anzubieten.

VERTRAUEN ALS ENTSCHEIDENDER ERFOLGSFAKTOR

Vertrauen ist auch bei der Armee und den Tätigkeiten der armasuisse zentral, und zwar in verschiedener Hinsicht. Einerseits, so Rüstungschef Martin Sonderegger, spiele das Vertrauen in langjährige Lieferanten bei der Beschaffung von Armeematerial eine wichtige Rolle. Andererseits sei es die Aufgabe der armasuisse, richtig zu antizipieren, welche Technologien, Materialien und Güter für den Schutz der Schweiz im Konfliktfall wann und wo benötigt werden. Dadurch fördere man das Vertrauen in die Sicherheit des Landes.



Sicherheitsdienste verkaufen, ohne Ängste zu schüren: Die Experten diskutieren Sicherheit als Business Case

Tests durchführen und in engem Kontakt mit Lieferanten stehen. Er betont, die Rekrutierung geeigneter Fachkräfte sei eine grosse Herausforderung, da man im Kampf um Talente einer starken Konkurrenz gegenüber stehe.

SICHERHEIT IST «SAFETY» UND «SECURITY»

Ein Zuhörer im Publikum bringt schliesslich einen weiteren Aspekt der Sicherheitsthematik auf. Er führt aus, Sicherheit werde stets als Abwehr gegen kriminelle Energie verstanden. Dies greife indes zu kurz, Sicherheit als Geschäftsfeld sollte sich nicht nur auf diese Art von Schutz beschränken. Er erwarte zum Beispiel Sicherheit bei Kindertagesstätten, bei der Spitex, in Altersheimen oder wenn er einen Aufzug benutze. So verstanden sei Sicherheit ein wesentliches Grundelement, damit die Gesellschaft in ihrer heutigen Form überhaupt funktionieren könne. Beat Glutz von Blotzheim geht mit der Wortmeldung einig und betont die Bedeutung des prophylaktischen Sicherheitsgeschäfts, das er einleitend als den Bereich «Safety» bezeichnet

gute Antwort darauf entwickelt. Diese Antwort bestehe nicht nur darin, die schädlichen Aktivitäten zu unterbinden. Man bietet den Kunden darüber hinaus die Möglichkeit, ihrerseits Sicherheit zu vermarkten, indem sie ihren Nutzern Spass an einer Technologie zur Wiedererkennung und am Umgang mit Originalen vermitteln.

Auch Hans Gut von der Hunkeler AG ist überzeugt, dass Angst keine Rolle spielen sollte. Nach seiner Erfahrung sind es oftmals Fehler, die dazu führen, dass ein Unternehmen ein Sicherheitsproblem erkennt und damit an einen Experten gelangt. Als Beispiel nennt er die kürzlich in den Medien thematisierten Fälle von falsch versendeten Kontoauszügen, welche die betroffenen Banken dazu veranlassen, nach

technischen Möglichkeiten zu suchen, um solche Fehler in Zukunft zu vermeiden.

«Angst ist ein schlechter Ratgeber», findet auch Securitas-Chef Beat Glutz von Blotzheim. Die Securitas habe noch nie Werbung mit der Angst gemacht und sei immer reaktiv auf Probleme eingegangen, die

Das Vertrauen in die Armee werde schliesslich auch durch viele weitere vertrauensbildende Massnahmen wie die Soforthilfe in Katastrophensituationen oder gerade während der Trockenperiode diesen Sommer bei der Wasserversorgung der Alpwirtschaften gestärkt. All diese Massnahmen und die Güter, die zum Wohl der Bevölkerung eingesetzt werden, schaffen laut Martin Sonderegger Vertrauen in die staatlichen Institutionen und deren Sicherheit.

DIE SCHWEIZ ALS IDEALER STANDORT

Die Schweiz, so sind sich die Podiumsteilnehmer einig, ist für das Sicherheitsgeschäft ein ausgezeichnete Standort. Pointiert bringt dies Hans Gut zum Ausdruck: «Wir könnten unsere Maschinen überall auf der Welt bauen lassen, aber wir wollen unsere Maschinen made in Switzerland. Wir brauchen immer bessere Leute, um uns ständig weiterzuentwickeln. Wir werden nie die Günstigsten auf dem Markt sein und können uns nur durch Innovation von unseren Mitbewerbern abheben. Und da sind wir in der Schweiz sehr gut aufgestellt.»



Thomas Villwock sieht grosse Marktchancen und viel Potenzial bezüglich Innovationen zur Verbesserung des Fälschungsschutzes

GEHEN WIR ZU SORGLOS MIT OFFENSICHTLICHEN RISIKEN UM?

Closing Key Note: Was bedroht die Schweiz? Eine sicherheitspolitische Lagebeurteilung aus Sicht des Nachrichtendienstes des Bundes.

Terrorismus, Spionage und Cyber-Angriffe gehören zu den zentralen Bedrohungen, mit deren Früherkennung und Bekämpfung sich der Nachrichtendienst des Bundes (NDB) tagtäglich befasst. Wie schätzt Paul Zinniker, stellvertretender Direktor, die momentane Sicherheitssituation in der Schweiz ein?

Die Frage nach einer Einschätzung der aktuellen Sicherheitslage in der Schweiz ist komplexer denn je. Eine Vielzahl von Akteuren und Risiken sind relevant und weltweite Entwicklungen müssen berücksichtigt werden. Die grössten Bedrohungen für die Sicherheit der Schweiz lassen sich in den Bereichen Terrorismus, Extremismus, Politik/Wirtschaft/Militär, Proliferation sowie im verbotenen Nachrichtendienst lokalisieren. Für Paul Zinniker stehen gegenwärtig die Themen Terrorismus, Cyber-Risiken und verbotener Nachrichtendienst im Vordergrund.

BEUNRUHIGENDE POLITISCHE ENTWICKLUNGEN IM AUSLAND

Verschiedene politische Entwicklungen werden von der Schweiz sorgfältig beobachtet: So erwähnt Paul Zinniker den Arabischen Frühling, die aktuellen Entwicklungen im Nahen Osten, die dadurch ausgelösten Migrationsströme und deren sicherheitspolitischen Aspekte. Weiter sieht er ein zunehmendes Ost-West-Konfliktpotenzial: Die Welt ist mit einem erstarkten Russland konfrontiert, das offenkundig Expansionsziele verfolgt. Für Europa stellt der Brexit eine Zerreissprobe dar und die Nato als zentrale sicherheitspolitische Organisation wird durch die von den USA verschärfte Lastenverteilungsdiskussion geschwächt. In all diesen politischen Entwicklungen zeigt sich laut

«Sie alle, die unternehmerisch tätig sind, können ein attraktives Ziel für ausländische Spionage sein. Deshalb gilt es, sich zu informieren und zu schützen.»

Paul Zinniker

Paul Zinniker, dass die Welt von Einzelpersonen regiert wird. Es sei eine Rückkehr der Grossmächte zu beobachten: «Die internationalen politischen Würfel sind von Führungspersonen und Nationalstaaten und nicht mehr von internationalen Organisationen und Bündnissen abhängig.» Gerade in diesem Zusammenhang müsse die Schweiz wachsam sein, damit sie nicht in diesen Strudel gerate.

CYBER-ATTACKEN ALS GROSSE GEFAHR

Im Zuge der Digitalisierung gewinnen Cyber-Bedrohungen an Bedeutung. Während die Polizei den Bereich der Internet-Kriminalität abdeckt, befasst sich der NDB mit der Spionageabwehr und mit einer weniger bekannten Form von Cyber-Attacken, den Angriffen durch Staaten.

Die Entwicklung des sogenannten «Internets der Dinge» führt zu einer zunehmenden Vernetzung von Geräten ohne besonderen Schutz. Dies macht kritische Infrastrukturen anfälliger für Angriffe.

Die Informationssicherheit, gibt Paul Zinniker zusammenfassend zu bedenken, umfasst eine private und eine geschäftliche Komponente. Jeder Einzelne müsse sich diesbezüglich fragen, wie er vorgehen wolle, wenn etwa ein Gerät sowohl privat wie auch geschäftlich genutzt würde. Selbst erfahrene Personen gingen mit diesen offensichtlichen Risiken erstaunlich sorglos um.

TERRORISMUS BLEIBT EIN THEMA

Hinsichtlich der Terrorismusgefahr ist die Schweiz zwar bis heute von Terrorakten verschont geblieben, dennoch ist diese Thematik in unserem Alltag präsent. Seit November 2015 stuft der NDB die Terrorbedrohung hierzulande als erhöht ein. Die grösste Gefahr gehe dabei nicht von Rückkehrern aus, sondern von Personen, die sich von Propaganda-Aktionen inspirieren liessen. So überwacht der NDB derzeit 585 Personen bzw. deren Aktivitäten im Internet und nimmt punktuell auch präventive Ansprachen vor. Als weitere Herausforderungen thematisiert Zinniker die Integration von zurückkehrenden Dschihad-Reisenden sowie den Umgang mit Terrorismus-Verurteilten nach verbüstem Strafvollzug.

SCHUTZ VOR SPIONAGE IST AUCH FÜR UNTERNEHMEN ZENTRAL

Die dritte zentrale Bedrohung, der verbotene Nachrichtendienst, ist laut Paul Zinniker die am wenigsten sichtbare unter den thematisierten Gefahren. «Aber ich habe diese Bedrohung noch nie so intensiv empfunden wie aktuell», sagt er, «gerade in Kombination mit Cyber-Aktivitäten wird in der Schweiz derzeit fast im Wochentakt staatlich motivierter Nachrichtendienst betrieben.» Eine besonders perfide Art von verbotenen Nachrichtendienst besteht darin, dass ausländische Mächte ihre Landleute in der Schweiz ausspionieren. Da die Betroffenen solche Akte aus Angst vor Repressalien gegen Angehörige nur selten an die Schweizer Behörden melden, gibt es hier gemäss Paul Zinniker eine hohe Dunkelziffer.



Paul Zinniker ortet im verbotenen Nachrichtendienst ausländischer Mächte in Kombination mit Cyber-Aktivitäten eine grosse Bedrohung für die Schweiz

Warum aber ist die Schweiz ein Ziel für Spionageangriffe ausländischer Staaten? Paul Zinniker betont, dass nicht in jedem Fall das Schweizer Staatswesen angegriffen werde. Häufig gehe es um Schweizer Institutionen oder um Daten, die hier gespeichert sind, um den Finanz- oder den Wirtschaftsplatz oder um Technologien und Know-How. Oft werde dabei die traditionelle Agentenspiegung mit digitaler Cyber-Überwachung verbunden. Aufgrund der prekären Risikolage hat der NDB ein Präventions- und Sensibilisierungsprogramm ausgearbeitet. Mittels einem Kurzfilm (<https://www.ndb.admin.ch/wirtschaftsspionage>) sollen besonders gefährdete Unternehmen, Institutionen und Bildungseinrichtungen sensibilisiert werden. Denn, so ist Paul Zinniker überzeugt, «Sie alle, die unternehmerisch tätig sind, können ein attraktives Ziel für ausländische Spionage sein. Deshalb gilt es, sich zu informieren und zu schützen.»

MODERNES NACHRICHTEN-DIENSTGESETZ BRINGT LICHT IN DIE «DUNKELKAMMER DER NATION»

Seine Ausführungen über die Sicherheitslage der Schweiz aus Sicht des Nachrichtendienstes führen Paul Zinniker abschliessend zur Organisation des NDB. Er betont, dass mit dem neuen Nachrichtendienstgesetz ein modernes Regelwerk geschaffen wurde, das die Kompetenzen des NDB ausweite und seine Arbeit erleichtere, aber gleichzeitig durch ausgebaute Genehmigungsverfahren und Aufsichtsorgane auch die Privatsphäre schütze. Früher habe man den NDB bisweilen als «Dunkelkammer der Nation» bezeichnet. «Ich kann Ihnen versichern», schliesst Zinniker, «im Zuge des neuen Gesetzes werden in dieser Dunkelkammer überall Neonröhren montiert, und das ist gut so.»

SICHERHEIT IST TEAMWORK – BEI PATROUILLE SUISSE IMMER!

Closing Key Note: Sicherheit, Verlässlichkeit und Vertrauen bei der Patrouille Suisse. Oder: die Zutaten für ein erfolgreiches Team an der Leistungsgrenze.



Der Kommandant der Patrouille Suisse, Nils Hämmerli «Jamie», misst den Ritualen unter den Piloten eine nicht zu unterschätzende Bedeutung bei

Sicherheit ist Teamwork – diesem Leitgedanken kommt bei der Patrouille Suisse eine überragende Rolle zu. Der Kommandant der Patrouille Suisse verrät, welche Eigenschaften ein Team braucht, um langfristig Topleistungen an der Leistungsgrenze zu erbringen.

Was ist eigentlich das Erfolgsrezept für eine gut funktionierende, erfolgreiche und leistungsstarke Truppe? Wie wählt man die richtigen Leute für ein solches Team und welche Rolle spielen Vertrauen, Rituale und Traditionen? Nils Hämmerli, der «Coach» der Jet-Kunstflugstaffel der Schweizer Luftwaffe, ist mitverantwortlich für die optimale Zusammensetzung seiner Mannschaft. Denn als Chef mit 26-jähriger Karriere bei der Luftwaffe muss «Jamie» – so sein Piloten-Spitzname – sicherstellen, dass seine Truppe auch nahe der Leistungsgrenze perfekt harmoniert. Das ist unabhängig: Praktisch Flügel an Flügel und mit Geschwindigkeiten von über 1'000 km/h donnern die Piloten der Patrouille Suisse bei ihren Formationsflügen durch den Himmel.

SICHERHEIT ALS OBERSTE PRIORITÄT

Kommandant Nils Hämmerli betont, dass die Patrouille Suisse Sicherheit kompromisslos als oberste Maxime verstehe. Daher gestaltet die Kunstflugstaffel ihre Formationen immer mit einer Sicherheitsmarge, die das Risiko minimieren soll. Schliesslich steht die Patrouille Suisse für Sicherheit, Präzision, Zuverlässigkeit und Leistungsbereitschaft und ihr Ziel ist es, diese typisch schweizerischen Tugenden im In- und Ausland zu demonstrieren.

«Vertrauen ist die Basis eines gut funktionierenden Teams.»

Nils Hämmerli

Diese Eigenschaften sind auch für die Piloten zentral, denn das Fliegen der Jets ist reine Handarbeit. Den Piloten stehen keine technischen Hilfsmittel wie GPS zur Verfügung, das Steuern bezeichnet Nils Hämmerli als «Sekundengeschäft». Die Entscheidungen eines Piloten haben im Verbandsflug immer einen direkten, unmittelbaren Einfluss auf die anderen Teammitglieder, so Hämmerli. Die Sicherheit wäre sofort gefährdet, wenn Regeln oder Absprachen, die zuvor im Team vereinbart wurden, nicht eingehalten würden. Deshalb ist Sicherheit bei der Patrouille Suisse zu jedem Zeitpunkt Teamwork.

DAS TEAM ALS SCHLÜSSEL ZUM ERFOLG

Der Erfolg der semi-professionellen Flugstaffel basiert auf einer einwandfrei funktionierenden Gruppe. Eine klare Hierarchie, offene Kommunikation, seriöses Training und eine starke Vertrauensbasis bezeichnet Nils Hämmerli als die Kernelemente seines Teams. Obschon die Piloten ein eigenes Cockpit haben, sitzen sie als Truppe schlussendlich im selben Boot. Erfolg kann in ihrem Beruf nur über die Gruppe definiert werden. Der hohe Stellenwert der Gruppe ist verantwortlich dafür, dass man sich bei der Patrouille Suisse nicht für ein Cockpit bewerben kann. Kandidaten werden ausnahmslos von der Gruppe ausgewählt. Stellt sich ein Mitglied mit seinem Vetorecht gegen einen Kandidaten, so ist eine Aufnahme in das Team ausgeschlossen. Als Chef der Gruppe achtet Nils Hämmerli aber sehr genau darauf, wie sich das Team zusammensetzt. Er setzt nicht auf bestimmte Stereotypen, sondern vielmehr auf einzelne Individuen mit unterschiedlichen Stärken und Schwächen. Die Fähigkeit, sich in eine Teambierarchie einzugliedern, ist dabei ebenso wichtig wie die Flugerfahrung.

sprechungen kämen heute im Berufsalltag nur selten vor, obschon sie für Unternehmen grosses Potenzial besässen.

TRADITIONEN UND RITUALE FÖRDERN TEAMGEIST

Neben den angesprochenen Attributen, spielen im Team der Patrouille Suisse Rituale seit jeher eine tragende Rolle. Jedes Neumitglied wird mit einer Taufe in die Gruppe aufgenommen. Solche Traditionen sollen die Zusammengehörigkeit, die Exklusivität und auch die Moral der Gruppe fördern. Sie sollen dabei helfen, ein Klima des Vertrauens zu schaffen.

Denn das Schaffen und Kultivieren einer Einheit lebt nicht selten von den einfachen Dingen. Ein beispielhaftes Ritual, das bei den Zuhörern für breites Gelächter sorgt, ist das konsequente Tragen von weissen Socken beim Fliegen. Vergisst ein Pilot diese Socken einmal zu Hause, muss er als Strafe barfuss in die Fliegerstiefel steigen. Aargauer hätten mit diesem Ritual wohl keine Probleme.

«Rituale und Traditionen fördern in einer Gruppe die Zusammengehörigkeit und die Moral.»

Nils Hämmerli

Der Hierarchie und dem Führungsstil spricht «Jamie» bei der Patrouille Suisse eine zentrale Rolle zu. So herrscht am Boden ein sehr kooperativer Führungsstil, jedes Teammitglied kann und soll gleichberechtigt seine Meinung äussern. In der Luft ändert sich dies radikal: Die Führung wird autoritär, der Leader der Flugstaffel übernimmt die Führung mit klaren Kommandos und Anweisungen. Das Debriefing nimmt als Führungsinstrument eine zentrale Rolle ein. Jeder Einsatz der Gruppe wird im Nachgang minutiös besprochen. Nils Hämmerli empfiehlt, solche Debriefings auch in Unternehmungen durchzuführen. Solche Einsatz-Nachbe-



Über Hierarchie und Führungsstil: Nils Hämmerli «Jamie»

DIE SCHWEIZ MUSS MOBIL UND WACHSAM BLEIBEN

Closing Key Note: Wir sind gefordert, die Sicherheit als Nährboden für den Schweizer Wohlstand zu erhalten.



Bundesrat Guy Parmelin identifiziert Terrorismus, Cyber Crime, Naturgewalten und bewaffnete Konflikte als die grössten Sicherheitsrisiken der Schweiz

Bundesrat Guy Parmelin erläutert die sicherheitspolitischen Konsequenzen, die aus den grössten Gefahren für die Schweiz – Bedrohung durch den internationalen Terrorismus, Gefahren aus dem Cyber-Raum, Gefahren durch Naturkatastrophen und bewaffnete Konflikte – hervorgehen und geht auf die angedachten Weiterentwicklungen der Landesverteidigung ein.

Bundesrat Guy Parmelin ist sich bewusst, dass die Zukunft und der Wohlstand der Schweiz auf der Dynamik und der Innovationskraft der Unternehmen beruhen. Damit einher geht die Verantwortung der Arbeitgeber. Zu dieser Verantwortung fühlt sich Guy Parmelin auch persönlich verpflichtet, schliesslich ist das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport VBS mit seinen rund 12'000 Mitarbeitenden selbst der grösste Arbeitgeber innerhalb der Bundesverwaltung und somit auch einer der grössten der Schweiz. Dank den finanziellen Mitteln, die der Verteidigung zur Verfügung stehen, ist das Departement zudem ein wichtiger Partner der Technologiebranche und der Industrie.

WAS SIND DIE GRÖSSTEN SICHERHEITSPOLITISCHEN GEFAHREN?

«Die Welt ist alles andere als ein Hafen des Friedens», mahnt Bundesrat Guy Parmelin.



Der Bundesrat ist überzeugt: Sicherheit geht nicht ohne Wirtschaft

Die sicherheitspolitischen Probleme sind nicht weit entfernt. Guy Parmelin denkt dabei an die Terroranschläge in Europa in den letzten Jahren, an die Konflikte in der Ukraine, an Cyber-Angriffe.

Der Bundesrat legt dem Parlament regelmässig seinen «Sicherheitspolitischen Bericht» vor. Im jüngsten Bericht aus dem Jahr 2016 stechen vier Gefahren besonders hervor. Ganz zuoberst figuriert der internationale Terrorismus. Er stellt in den Augen des Bundesrats die grösste Bedrohung dar. Die Gefahr ist an sich nicht neu, doch sie hat in den letzten drei Jahren erheblich zugenommen. Seit Januar 2015 sind in Westeuropa rund 350 Menschen bei Terroranschlägen getötet und rund 1'500 verletzt worden. Das sollte zur Vorsicht mahnen.

Es gilt, die nachrichtendienstlichen Tätigkeiten in Koordination mit den Kantonen, den grossen Städten und unseren internationalen Partnern fortzuführen. Denn die Gefahr, die von radikalisierten Einzelpersonen oder Gruppen ausgeht, besteht weiter, auch wenn der Islamische Staat heute besiegt scheint. Eine zweite Gefahrenquelle betrifft den Cyber-Raum. Der Bundesrat

hat kürzlich seine «Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken 2018–2022» erarbeitet. Aus dieser Strategie geht eine neue spezifische Aufgabe des VBS hervor, die sogenannte «Cyber-Defence». Dabei geht es um den Schutz der VBS-eigenen Infrastrukturen wie beispielsweise der IT-Systeme der Armee oder um nachrichtendienstliche Massnahmen. Selbstverständlich unterstützt das VBS auch die zivilen Behörden, wenn kritische Infrastrukturen ins Visier von Angriffen geraten. «Aber es liegt an allen, aufmerksam zu sein – auch an den Unternehmerinnen und Unternehmern», appelliert Guy Parmelin an die Zuhörer im Saal. Auch KMUs seien keinesfalls sicher vor den Gefahren aus dem Cyber-Raum. Nicht alle Unternehmen seien sich der Risiken bewusst, dabei sei es entscheidend, dass alle Wirtschaftsakteure die Risiken erkennen, die eigenen Risiken überprüfen und sich entsprechend schützen würden.

Nach dem Terrorismus und Gefahren aus dem Cyber-Raum geht Guy Parmelin drittens auf Naturkatastrophen und Notlagen wie Pandemien ein. Besonders extreme Naturereignisse treten in jüngerer Vergangenheit häufiger auf. So stellt sich heutzutage nicht mehr die Frage, ob eine Naturkatastrophe eintritt, sondern viel eher wann und in welchem Ausmass. Insbesondere Überschwemmungen, Erdbeben und Murgänge zählen zu den realistischen Bedrohungen.

Terrorismus, Cyber-Risiken, Naturgefahren – neben diesen drei komplexen Bedrohungen muss nach wie vor auch ein konventioneller bewaffneter Konflikt als mögliches Risiko betrachtet werden. Allerdings zählen eine strategische Bombardierung oder eine Panzeroffensive heute nicht mehr zu den zentralen Szenarien des VBS. Obwohl ein herkömmlicher bewaffneter Konflikt in der Schweiz in der heutigen Ausgangslage nicht wahrscheinlich scheint, weiss niemand, wie die Situation in zehn oder zwanzig Jahren aussehen wird.

DIE SICHERHEITSPOLITIK MUSS SICH WEITERENTWICKELN

An den europäischen Aussengrenzen bestehen dauerhafte Spannungsherde. Es ist nicht vollständig auszuschliessen, dass sich diese ausdehnen und die Schweiz eines Tages direkt betreffen. Daraus folgt, dass sich die Sicherheitspolitik notwendigerweise kontinuierlich weiterentwickeln und man die Verteidigungsmittel anpassen muss. Um sich diesen veränderten Gegebenheiten anzupassen, durchläuft die Armee derzeit eine wichtige Reform, die «Weiterentwicklung der Armee» (WEA). Kernpunkte der WEA sind Verbesserungen in der Bereitschaft, in der Ausbildung und in der Ausrüstung sowie eine stärkere regionale Ausrichtung.

Guy Parmelin äussert sich auch zu Air2030, das heisst zur Beschaffung neuer Kampfflugzeuge und eines Systems der bodengestützten Luftverteidigung grösserer Reichweite (Bodluf). Dieses Thema ist aus zwei Gründen wichtig. Erstens ist es von direktem wirtschaftlichen Interesse, denn



Sichtlich gut gelaunt geniesst Bundesrat Guy Parmelin zum ersten Mal den Pilatus

die ausländischen Auftraggeber werden via Offsets Aufträge für mehrere Milliarden Franken in der Schweiz platzieren müssen. Zweitens vernimmt man derzeit einige Kritik an dem vom Bundesrat vorgeschlagenen Vorgehen: Referendum oder kein Referendum, Flugzeuge und Bodluf als Paket oder einzeln? Er selbst hält es für sinnvoll, ein Referendum über die Beschaffung von Flugzeugen und Bodluf als Paket zu ermöglichen. Seines Erachtens ist ein Planungsbeschluss des Parlaments der beste Weg dazu.

Zur Begründung führt er drei Argumente auf: Erstens bestehen demokratische Erwartungen, denn auch über die letzten beiden Vorhaben zur Beschaffung von Kampfflugzeugen wurde abgestimmt. Auch wenn die Präzedenz keine rechtliche Verpflichtung schafft, ergibt sich daraus doch eine politisch relevante Erwartungshaltung. Das zweite Argument ist die Planungssicherheit: Das Vorhaben wird sich bis zum Abschluss der Einführung der zu beschaffenden Systeme über rund zwölf Jahre hinziehen. Diese lange Zeitspanne und das beträchtliche finanzielle Engagement verlangen so viel Planungssicherheit wie möglich. Der Planungsbeschluss des Parlaments ist ein geeignetes Mittel dazu. Drittens besteht bei einem referendumsfähigen Planungsbeschluss mehr Kontrolle über die konkrete Formulierung des Beschlusses und dessen Zeitplan, als wenn auf eine Volksinitiative reagiert werden müsste, über deren Zeitplan und Wortlaut andere bestimmen. Eine Volksinitiative nach einem Referendum ist zwar möglich, wäre politisch aber eher schwer zu begründen. Der Bundesrat wird nach Ende der Vernehmlassung entscheiden, wie er weiterfahren will. Doch man ist sich bewusst, dass es für Air2030 eine breit abgestützte, tragfähige Basis braucht.

Weiter erwähnt Guy Parmelin auch die voraussichtlichen Kompensationsgeschäfte. Sie verteuern zwar die Beschaffung, aber dafür gibt es eine Gegenleistung. Die Industrie wird gestärkt, aber nicht nur sie allein. Arbeitsplätze werden geschaffen und erhalten. Unternehmen erhalten Zugang zu Know-How, das ihre Zukunftsfähigkeit verbessert, und auch Zugang zu neuen Märkten. Bund, Kantone und Gemeinden gewinnen durch ein höheres Steueraufkommen.

DIE NOTWENDIGKEIT MODULARER LÖSUNGEN

Die Grundpfeiler unserer nationalen Sicherheit haben sich ebenso verändert wie die grössten Bedrohungen. Es braucht modulare Lösungen. Die Armee ist in Zukunft nicht mehr zwingend die Speerspitze der Nation im Kampf gegen Angriffe. Krisensituationen verlangen in Zukunft nicht immer rein militärische Antworten. Aber solche werden immer häufiger erforderlich sein.

Die Fähigkeit zur Zusammenarbeit spielt unter diesen Umständen eine entscheidende Rolle. Guy Parmelin denkt dabei an Partner-Staaten, Kantone, Städte, ebenso wie die Betreiber kritischer Infrastrukturen. Und nicht nur die öffentliche Hand, auch die privaten Unternehmen sind gefordert. Sicherheit geht nicht ohne die Schweizer Wirtschaft. Gemeinsam können die Bedrohungen eingeschätzt und

gemeinsam sollen Lösungen gefunden werden, die aufeinander abgestimmt sind. Guy Parmelin sieht die Sicherheitspolitik als eine Verbundsaufgabe, erst recht in einem föderalistischen Land wie der Schweiz. Erfreulicherweise gelingt das bislang ausgesprochen gut. Gemäss der Jahresstudie «Sicherheit» der ETH Zürich fühlen sich 95 Prozent der hiesigen Bevölkerung sicher. Das liegt auch an der stabilen Entwicklung der Schweiz und am Wohlstand. Doch dieses Sicherheitsgefühl ist nicht auf Dauer gegeben oder garantiert. Man muss es stetig erneuern und bestätigen. Und man muss sich bewusst sein, dass Sicherheit ein nie zu erreichendes Ideal darstellt.

Nach der Ansicht von Bundesrat Guy Parmelin muss die Schweiz mobil und wachsam bleiben. Wenn das gelingt, bleibt die Sicherheit als Nährboden erhalten, auf dem wirtschaftlicher Erfolg und individueller Wohlstand gedeihen können.

TB

«Die Welt ist alles andere als ein Hafen des Friedens.»

Guy Parmelin



Die IHZ erfüllt jeden Wunsch: Brigit Fischer bringt dem Bundesrat den gewünschten Kaffee



Einmal mehr: Das Wirtschaftsforum 2018 vor vollen Rängen

IMPRESSIONEN VOM PILATUS



IHZ-Vorstandsmitglieder Ralph Müller, SCHURTER Holding AG, Peter Galliker, Galliker Transport AG, und Beat Wullschleger, Wilhelm Schmidlin AG



Silvia Rose von der Gesellschaft der St. Anna Ärzte Luzern im Gespräch mit Susanna Auf der Maur und Markus Kaufmann von Kaufmann Rüedi Rechtsanwälte



Thomas Affolter, KPMG, interessiert sich für die Ausführungen von Philipp Meier, Apostroph Luzern AG



Scheinen sich gut zu amüsieren: Regierungsrat Daniel Wyler und Nationalrätin Yvette Estermann



Auf dem Weg zu den Opening Key Notes: IHZ-Vorstandsmitglieder Felix Meyer, Genossenschaft Migros Luzern, und Istvan Szalai, Garaventa AG



Ueli Kürschner, A4 Agentur, und das Löwenfels-Team mit Oliver Meyer, Karin Werner und Walter Capozzolo im Austausch mit Felix Howald, IHZ



Auf direktem Weg von Bundesbern ans Wirtschaftsforum auf dem Pilatus: Bundesrat Parmelin im Anflug



Bundesrat im überparteilichen Gespräch mit den Luzerner Bundesparlamentariern Damian Müller, Konrad Graber und Franz Grüter



Regierungsräte Andreas Barraud, Schwyz, und Marcel Schwerzmann, Luzern, mit HSLU-Rektor Markus Hodel



Das Programm ist zwar spannend und wichtig, die Networking Breaks aber mindestens ebenso. Und die Pilatus-Terrasse lädt zum Verweilen ein...



Kurze Stärkung: IHZ-Vorstandsmitglied Brigitte Breisacher, Alpnach Norm-Holding AG, beim Lunch mit Thomas Wirth, wirth+co ag



Stefan Keller, Bataillard AG, diskutiert mit IHZ-Vorstandsmitglied Marion Klein, PACK EASY AG



Kamen beide zu Fuss auf den Pilatus: Karin Auf der Maur, admind public relations, und IHZ-Vorstandsmitglied Silvan Felder, Verwaltungsrat Management AG



Gibt jedes Mal wieder einen würdigen Rahmen für das Farewell Dinner: Der Victoria-Saal des Hotel Pilatus Kulm



«C'est le ton qui fait la musique.» Bruno Bieri verzaubert mit seiner Hang

PARTNER

Strategische Partner



Forum Partner



Knowledge Partner



Wirtschaft
FH Zentralschweiz

Medien Partner



Event Partner



Das Zentralschweizer Wirtschaftsforum wird unterstützt durch die Zentralschweizer Kantone.

IMPRESSUM

Herausgeberin
Industrie- und Handelskammer
Zentralschweiz IHZ
Kapellplatz 2, 6002 Luzern

Koordination und Design
Leitung: Brigit Fischer
Inserate: IHZ und Peter W. Ottiger
Gestaltung: thomagrafik.com
Lektorat: Lisa Kneubühler

Text Hochschule Luzern – Wirtschaft
Thomas Birrer, TB
Brian Mattmann, BM
Isabelle Oehri, IO

Text IHZ
Felix Howald, FH

Fotografie
Ben Huggler Photography
www.benhuggler.ch

Druck
Brunner Medien AG
Arsenalstrasse 24
CH-6011 Kriens



printed in
switzerland