Eröffnung Mittwoch 17. November 2021

9.30 – 10.20 Uhr

Rainer Maria Salzgeber
Moderation und Eröffnung des Symposium

Keynote von Nicolas Bürer – CEO digitalswitzerland
Zukunft und Chancen der digitalen Innovation
Nicolas Bürer ist seit 2016 Geschäftsführer von digitalswitzerland. Zuvor war er in verschiedenen Positionen bei Deindeal.ch, Movu und dem ehemaligen TV-Sender Joiz Schweiz tätig. Er studierte Physik an der École polytechnique fédérale de Lausanne (EPFL).
Im Jahr 2018 wurde Nicolas Bürer als „Swiss Business Angel of the Year" ausgezeichnet. Er ist ein leidenschaftlicher Unternehmer und Startup-Investor.
Digital ist das Thema der Stunde. Die Pandemie hat die digitale Innovation um ein Jahrzehnt vorangebracht. Mit welchen Risiken und Chancen und daraus abgeleiteten Hypothesen werden wir in den kommenden Jahren konfrontiert sein?

Natalie Gratzer – Bundesamt für Wirtschaftliche Landesversorgung, BWL
Nathalie Gratzer ist seit 2020 Projektleiterin zur Umsetzung der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) im Bundesamt für Wirtschaftliche Landesversorgung. Sie entwickelt Cybersicherheits Empfehlungen des Bundes für kritische Infrastrukturen und leitet die Gefährdungsanalyse der wirtschaftlichen Landesversorgung 2021. Der Erwerb ihres Master of Science in Business Information Systems entfachte ihre Begeisterung für Cybersicherheit und Krisenmanagement. Nathalie engagiert sich gerne in Cybergremien und strebt aktuell ihre CISSP Zertifizierung an, um leidenschaftlich die Cyberwelt mitzugestalten.

Open Forum Mittwoch 17. November 2021

11.00 – 11.40 Uhr

Sarah Mühlemann – Präsidentin, Digital Self Defense Foundation

Vom Wissen zum Handeln mit Incentivized Security Awareness

Oft schaffen wir mit Security Awareness zwar ein Gefahrenbewusstsein, doch die eigentlich angestrebte Veränderung im Sicherheitsverhalten bleibt aus. In diesem Referat erhalten Sie einen praxisnahen Einblick in den Ansatz des Incentivized Security Awareness als Katalysator für den Wandel vom Wissen zum Handeln.

14.00 – 14.40 Uhr

Jens Henkner – CEO von CertX

Neue Cybersicherheitsvorschriften oder wenn Zertifizierungen als Market Enabler genutzt werden:

Die Paradigmen der Systemzulassung und Homologation verändern sich derzeit in fast allen Industriebereichen. Die zunehmende Vernetzung, die wachsende Komplexität sowie der Einsatz neuer Technologien wie Machine Learning zwingt die Behörden dazu, ihre bisherigen Genehmigungssysteme anzupassen und neue Anforderungen zu integrieren, wo die Dimensionen der Cybersicherheit auftauchen. Einführung in die verschiedenen Ebenen von Anforderungsorganisationen, mit denen sich Organisationen auseinandersetzen müssen, und wie technische Standards als wichtige Referenzen verwendet werden könnten, um ihre Übereinstimmung mit dem Stand der Technik nachzuweisen. Um aufschlussreicher zu sein, werden der Automobilsektor und die Homologation von Strassenfahrzeugen als echtes Beispiel für die Auswirkungen von Cybersicherheitsanforderungen auf etablierte Lieferketten verwendet.

15.00 – 15.40 Uhr

Nick Mayencourt – Global CEO, Dreamlab Technologies AG

Cybergedon - die fünfte Dimension

Cybersecurity, wie physische Security verfolgen die bestmögliche Abschottung gegen Gefahren. Während physische Grenzen bekannt und gut beherrscht werden, stellt die cyberphysische Dimension neue, vom Menschen geschaffene Herausforderungen dar. Dies wird anhand der Veränderung des Schweizer Cyberraums der letzten Jahre aufgezeigt

TRACK 1 Mittwoch 17. November 2021

Raum: B

10.20 – 11.00 Uhr

Patrik Kamber – Program Manager Digital Solutions, Johnson Controls

Früherkennung von Gefahrenzusammenhängen

Vorstellung einer Plattform, die darauf ausgelegt ist Menschen, Assets, Institutionen und Unternehmen zu schützen. Das System untersucht kontinuierlich interne und externe Datenquellen, korreliert und klassifiziert Bedrohungsdaten und berechnet dann die Auswirkungen der Bedrohungen

11.20 – 12.00 Uhr

Fabio Lo Curto – Country Manager Hospitality, SALTO Systems AG

Self Check In von heute

Für Reisende und Gäste ist ein reibungsloser Self Check-In essentiell. Insbesondere dann, wenn man eine kontrollierte und überwachte Zugangskontrolle ohne Personal anbieten will und gleichzeitig auch die aktuellen COVID Schutzmassnahmen auf einen Nenner vereinen möchte. Sämtliche Abläufe werden beschleunigt und tragen zudem zur Sicherheit für den Betreiber, aber auch der Gäste bei.

Raum: C

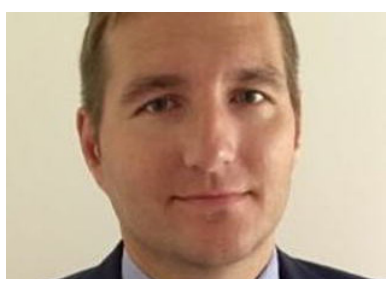
10.20 – 11.00 Uhr

Christophe Monigadon – Leiter Informationssicherheit, Berner Kantonalbank

Wofür brauchen wir eine IT Sicherheitskultur? Wir haben doch eine Firewall!

Technische Sicherheitsvorkehrungen reichen im Kampf gegen die Cyberkriminalität nicht aus. Die Cyber Resilienz eines Unternehmens hängt auch stark von ihrer IT-Sicherheitskultur ab. Doch wie entsteht eine nachhaltige Sicherheitskultur?

11.20 – 12.00 Uhr



Roman Stefanov – Head CyberSecurity Sales Cisco Switzerland

Effektiver Cybersecurity Schutz – für die Bedrohungen von heute und morgen

Um sich wirksam vor Cyberangriffen zu schützen, reichen wenige, nicht integrierte Produkte schon lange nicht mehr aus. Ein ganzheitlicher Plattformansatz ist die Securityarchitektur der Zukunft. Wir beleuchten in diesem Vortrag, welche Vorteile eine integrierte, offene Plattform bietet und wie diese aktuelle Trends wie Zero Trust und SASE abbildet.

TRACK 3 Mittwoch 17. November 2021

Raum: B

13.20 – 14.00 Uhr

Urban Stenz – Geschäftsführer, EVVA Sicherheitstechnologie AG

Das smarte Türschloss

Elektronische Schlüsselvergabe per Smartphone, Navigation vor die Haustüre und weitere Integrationsmöglichkeiten der Zutrittskontrolle in Drittsysteme.

14.20 – 15.00 Uhr

Christoph Widler – Gründer & VRP, TeleConex AG

Zutritt und Werkschutz in Kombination mit Gebäudeinformatik-Systemen in hybriden Umgebungen

Digitalisierung unterstützt uns über alle Branchen – doch Gebäudesicherheit und Werkschutz hinken aktuell noch etwas hinterher: Für Gebäudebetreiber ist das Verwalten von physischen Zutrittsmedien eine Qual. Im Zeitalter von Smart Buildings muss das nicht sein.

15.20 – 16.00 Uhr

Rinaldo Zanella – Mitgründer und CEO, Trigon AG

Prävention durch Information!

Mit der Überwachung der Infrastruktur wie Gebäude Areale, ja ganze Gemeindegebiete, erhält man online den Status oder die Alarme bei Veränderung und kann agieren/reagieren. Unerlaubter Zutritt in Gebäude, auf Areale oder auf Baustellen werden sofort detektiert. Wassereintritt, hohe Windgeschwindigkeiten oder andere Ereignisse die zu Schäden führen können, werden angezeigt.

16.20 – 17.00 Uhr

Michael Dudli – CEO, Xelon AG

Dedicated Cloud Infrastructure as a Service

Nachdem die digitale Transformation eine regelrechte Migrationswelle von On Premise Infrastruktur in die Cloud verursacht hat, stellen sich viele Firmen hinsichtlich der langfristigen, strategischen Planung die Frage, wie die Restriktionen und Bedenken bei Themen wie Sicherheit, Compliance oder Kosten entschärft werden können. Das Referat zeigt die Lösung auf.

TRACK 4 Mittwoch 17. November 2021

Raum: C

13.20 – 14.00 Uhr

Dr. Lukas Ruf – Group CISO, Head CU Security&Risk, Migros-Genossenschafts-Bund

Cyber Security – eine wesentliche Schutzmassnahme zur Sicherung der Business Continuity

Cyber Security ist eine der wesentlichen Schutzmassnahmen, welche die Migros gegen Angriffe aus dem Cyber-Space schützt. Im Referat wird die Organisation und die Einbettung der Cyber Security im Rahmen des IT Service Continuity Managements vorgestellt.

14.20 – 15.00 Uhr

Prof Dr Marc K Peter – Global Transformation Leader, Hochschule für Wirtschaft FHNW

Homeoffice und Cybersicherheit in Schweizer KMU

Im ersten Lockdown im März/April 2020 hat sich die Zahl der Mitarbeitenden, welche von zu Hause arbeiteten, fast vervierfacht. Die Themen zur Digitalisierung, zum Home-Office, dem Einsatz von Informations-Technologien und zur Cyber-Sicherheit haben im Umfeld von Corona / COVID-19 an Wichtigkeit gewonnen.

15.20 – 16.00 Uhr

Urs Achermann – Director, Business Development Kudelski

Cyber Angriff Ransomware - Lösegeldverhandlung - Worauf muss ich bei einer Verhandlung achten?

Wir sind mit vielen CISOs und CIOs in der Schweiz in Kontakt und eine Frage tauchte immer wieder auf: «Wenn ich Opfer einer Ransomware Attacke werde, dann zahl ich einfach, da ich eine Cyber Versicherung habe.» Aber ist das im Ernstfall so einfach? Die Angriffsaktivitäten der Gruppe DarkSide, die auch für den Angriff auf die Colonial Pipeline zuständig war, gaben einen Einblick in die Verhandlungen, der sich mit unseren eigenen Erfahrungen deckt.

16.20 – 17.00 Uhr

Candid Wüest – VP Cyber Protection Research, Acronis

Verschmelzende Cyberkriminalität – Gefahren-Trends am Horizont

Cyberkriminelle kombinieren vermehrt Methoden für eine maximale Erfolgschance. Der Trend zeigt eine weitere Verschmelzung und Automatisierung der Angriffe um deren Effizienz und Profitabilität noch weiter zu steigern. Anhand von konkreten Vorfällen zeigen wir, wie sich diese kombinierten Gefahren-Trends auszeichnen und wieso ein integrativer Schutz und verbesserte Visibilität nötig ist.

Open Forum Donnerstag 18. November 2021

9.30 – 10.10 Uhr

Sandro Nafzger – CEO & Co Founder, Bug Bounty Switzerland

Zusammenarbeit mit ethischen Hackern. Der Schlüssel damit Ihre digitale Transformation gelingt

Um sich effektiv vor Cyberattacken zu schützen, führt kein Weg an der Zusammenarbeit mit ethischen Hackern vorbei. Wie Sie dadurch Security Excellence erreichen und sicherstellen, dass Ihre digitale Transformation gelingt, erfahren Sie in diesem spannenden Talk anhand konkreter Praxisbeispiele.

11.00 – 11.40 Uhr

Sabine Fercher – Gründerin, Fercher Compliance GmbH

Datenschutz verkauft Sicherheitsdienstleistungen und –produkte

Governance und Compliance - Einblicke in die Anforderungen der Datenschutz-Grundverordnung an Corporate Digital Security. Können Sie Ihre Sicherheitsdienstleistungen oder -produkte mit diesen Erkenntnissen verkaufen?

15.00 – 15.40 Uhr

Natalie Gratzer – BWL

Cyber-Risiken als Bedrohung für kritische Infrastrukturen und das Funktionieren der Schweiz

Die Schweiz ist auf das reibungslose Funktionieren der kritischen Infrastrukturen angewiesen. Mit der zunehmenden Vernetzung digitaler und physischer Systeme nehmen die Chancen, im Gleichschritt zu den Cyber-Risiken, zu. Wie können wir sicherstellen, dass Kritische Infrastrukturen Cyber-Bedrohungen erkennen und bekämpfen und sie unterstützen, widerstandsfähiger zu werden?

16.00 – 16.40 Uhr

Markus Kaegi – Senior Strategic Sales Consultant, Lead Cyber Security, UMB AG

Das Internet ist zum Klicken da! Warum wir mehr Klicken sollten und trotzdem sicher sind

Welche Eckpfeiler sind zentral, um eine hohe Cyber Sicherheit zu erreichen. „Mit Vorsicht klicken" oder «weniger klicken» ist zu kurz gedacht. In einer digital und agilen Welt gilt es ein ganzes Eco-System zu kennen und vielmehr zu beeinflussen. Wir betrachten und priorisieren an diesem Referat die Stellschrauben für eine hohe Cyber Security Maturität.

SMIDEX SUISSE – Programmänderungen möglich und vorbehalten

Raum: B

10.20 – 11.00 Uhr

Mischa Kemmer – Bank Julius Bär AG, Information Security, Head Awareness and Consulting

Cyber security starts with you!

Die Mitarbeitenden eines Unternehmens sind die erste Verteidigungslinie im täglichen Kampf gegen Cyber-Attacken. Eine clevere, durchdachte Awareness-Kampagne trägt zur Stärkung des individuellen Verantwortungsbewusstseins bei, damit nicht nur die Unternehmung, sondern auch alle Mitarbeitenden in ihrem eigenen, privaten Umfeld geschützt sind.

11.20 – 12.00 Uhr

Aarno Aukia – CTO, VSHN The DevOps Company

DevOps und DevSecOps im Einsatz im Schweizer Banking

Aarno stellt die Secure Banking Operation Platform vor, die auf DevOps in Entwicklung und Betrieb basiert: Agile Entwicklungsprozesse, Container-Plattformen und Tools für das operative Security Engineering sind Kernthemen. Auf der Seite des Technologiepartners liegt der Fokus auf der DevOps-Pipeline und -Technologie, auf der Seite der Kernbankenapplikationen auf den Erfahrungen beim Aufbau dieser Systeme, dem Testen und dem Umgang mit Risikobewertung und Sicherheitsfragen.

Raum: C

10.20 – 11.00 Uhr

Ruedi Moll – CuriX

AI basierte Immunabwehr für IT-Systeme

Grundlage für zunehmend digitalisierte Geschäftsprozesse sind widerstandsfähige Systeme – gegen Angriffe von aussen sowie gegen Fehler innerhalb eines Systems. CuriX ist ein NextGeneration-Tool, das auf Basis von AI permanent den Blick nach innen und aussen richtet. Verdächtige Muster werden so vollautomatisiert erkannt gebündelt («noise redcution») und bekämpft; potenzielle Incidents werden vorhergesagt und System-Ausfälle können so verhindert werden, bevor diese etwa von einem Monitoring oder SIEM-Tool überhaupt im Ansatz erkannt werden; Angriffe - auch unbekannter Art - werden im Keim erkannt und erstickt. CuriX dokumentiert zudem lückenlos und zeigt Schwachstellen auf, bevor diese zum Leck oder Problem werden: «all you need to be compliant».

11.20 – 12.00 Uhr

Levente J. Dobszay – Cybersecurity Specialist, Electrosuisse

Cybersicherheit braucht Regeln

Betreffend Cybersicherheit besteht eine «Transformationslücke» in der Digitalisierung. Da bisher weder die Hersteller und Dienstanbieter, noch die Anwender wirksame Sicherheitsstandards etablieren konnten, muss von einem Marktversagen hinsichtlich der Cybersicherheit gesprochen werden. Die digitale Welt benötigt gesetzlich verankerte Mindestsicherheitsstandards.

Raum: B

13.20 – 14.00 Uhr

Thomas Gusset – CEO/CTO NetSec.co AG

One Client Strategie mit Windows Bordmitteln umsetzen

Ein zweites Gerät für die Nutzung im Homeoffice ist aufwändig und teuer, der Einsatz privater Geräte verbietet sich eigentlich aus Sicherheitsgründen. In der Fallstudie wird aufgezeigt, wie man mit Windows Bordmitteln (AoVPN, RRAS, Windows Firewall) einen mobilen Windows Client bauen kann, der komfortabel und sicher sowohl im Büro als auch im Homeoffice verwendet werden kann.

14.20 – 15.00 Uhr

Marco Hiestand – CEO, BREVIT AG

Einfache, umfassende und bezahlbare Cybersecurity-Lösungen für Schweizer KMU

Wie gut ist Ihr KMU eigentlich vor Cyberangriffen geschützt? Wir stellen ein modulares 360° Cybersecurity-Modell vor, welches Schweizer KMU einfach, umfassend und bezahlbar vor Cyberrisiken schützt. Das Referat vermittelt die Inhalte einfach und verständlich aus einer Managementperspektive.

15.20 – 16.00 Uhr

Robin Campbell – Ironnet

Infos folgen.

16.20 – 17.00 Uhr

Mischa Obrecht – Cyber Security Specialist , Dreamlab Technologies AG

KI für Cyber Security - Traumpaar oder Wunschdenken?

Künstliche Intelligenz (KI) und Machine Learning Techniken werden häufig als Allheilmittel gegen Bedrohung der Cyber Security angepriesen. Besserer Schutz? KI. Mehr Automatisierung? KI. Mehr Überblick? KI. Mehr Zuverlässigkeit? KI. Mit diesem Vortrag wagen wir einen kritischen Blick darauf, wie und wo KI diesen Erwartungen gerecht werden kann und wo nicht.

Raum: C

13.20 – 14.00 Uhr

Andreas Plüer – lic. oec. HSG, Bereichsleiter Digital Services, EKT AG

Erfahrungsbericht Cyberattacke – sprechen wir Klartext!

Andreas Plüer durchlebte selbst die Auswirkungen eines dramatischen Cyberangriffs und berichtet heute über seine Erfahrungen. Er spricht Klartext über die Angreifer und ihr Vorgehen, über seine Fehleinschätzungen im Vorfeld der Attacke und empfiehlt wirksame Schutzvorkehrungen vor Cyberangriffen.

15.20 – 16.00 Uhr

Frederic Buchi – Senior Security Consultant, Siemens Schweiz AG

Zero Trust – die IT/OT-Annäherung und die sich ständig verändernde Bedrohungslandschaft erfordern einen neuen Ansatz für Sicherheit und Vertrauen

Traditionelle IT/OT-Umgebungen werden wie eine sichere Festung geschützt – alles innerhalb des Netzwerks gilt als vertrauenswürdig, alles ausserhalb als feindlich, wobei Firewalls die Rolle eines Torhüters spielen, der Entscheidungen basierend auf IP-Adressen und Ports trifft.
Dieser Ansatz stösst zunehmend an seine Grenzen in einer Zeit, in der die meisten Mitarbeiter remote arbeiten und industrielle Steuerungssysteme zunehmend mit der Cloud verbunden sind, so dass zusätzliche Sicherheitskontrollpunkte ausserhalb des Netzwerks erforderlich sind.
Bei Zero Trust wird kein Gerät, kein Benutzer und kein System standardmässig als vertrauenswürdig angesehen – weder innerhalb noch ausserhalb des Unternehmens/Netzwerks.
In dieser Präsentation stellen wir die zentralen Konzepte hinter Zero Trust vor und wie diese bei industriellen Systemen angewendet werden können.

Raum: C

14.20 – 15.00 Uhr

D. Schmutz

P. Zumstein

Daniel Schmutz – Head of Channel & Marketing ALPS, Trend Micro (Schweiz) GmbH
Bruno Buser – CFO & Mitglieder der Geschäftsleitung, Stöcklin Logistik AG
Patrick Zumstein – Leiter IT-Infrastructure, Fachhochschule Nordwestschweiz (FHNW)

Der Angriff kommt – aber was dann? Interview mit zwei Vertretern bekannter Schweizer Unternehmen.

Schreckensnachricht Cyber-Angriff – Alarmstufe Rot. Was läuft, nachdem die Attacke entdeckt wurde, überhaupt in einem Unternehmen ab? Welche Sofortmassnahmen müssen getroffen werden? Wer informiert wen, wann und in welcher Kadenz über die Schritte?

16.20 – 17.00 Uhr

Daniel Nussbaumer – Dr. iur., Leiter Cyber Security, T-Systems Schweiz AG

Cyberangriffe auf Verkehrsmittel

Die Art und Weise, wie Unternehmen sich und ihre Produkte gegen Cyberkriminalität schützen, ist höchst individuell. Gleichzeitig finden Cyberkriminelle immer neue Wege um möglichst viel Schaden anzurichten. Zu einem angemessenen Schutz vor Cyberkriminellen gehört heute nicht nur die Absicherung der IT, sondern der Schutz sämtlicher Geräte, welche durch Cyberkriminelle angegriffen werden können, also neben Autos auch Züge oder Flugzeuge.