IDSF-Initiator Helmut Leopold, AIT und Martin Szelgrad, Report Verlag, eröffneten das internationale Forum zum Thema Digitalisierung & Sicherheit.

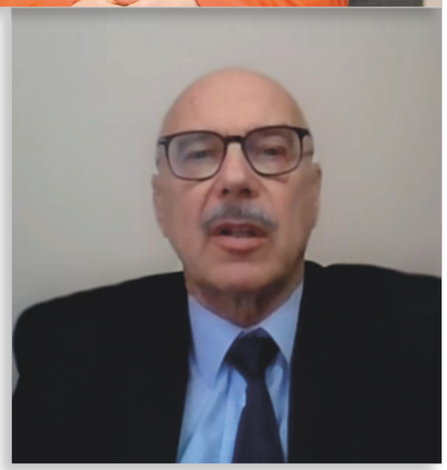
Mariana Kühnel, Wirtschaftskammer Österreich: »Die Digitalisierung birgt Chancen, aber auch Herausforderungen, etwa in Form von Cyberangriffen.«

»Wollen die digitale Welt zu einem erfreulichen und sicheren Ort machen«

Herausforderung für die vernetzte Gesellschaft und Wirtschaft: Beim International Digital Security Forum (IDSF) in Wien wurde ein globaler Dialog zur Erhöhung der Sicherheit initiiert.

VON MARTIN SZELGRAD

Die Corona-Pandemie legt schonungslos Schwachstellen unseres Gesellschafts- und Wirtschaftssystems offen. Das betrifft auch die Abhängigkeiten, die im Zuge der Digitalisierung entstanden sind. Digitale Infrastrukturen wie beispielsweise Social-Media-Plattformen, Videokommunikationssysteme, aber auch Behördennetzwerke und Bürgerservices, digital vernetzte Fabriken, Dateninfrastrukturen im Gesundheitswesen, die Energieversorgung und Telekommunikation, bis hin zur intelligenten Haussteuerung – all das muss zuverlässig funktionieren. Funktionieren, das heißt heute auch, resilient gegenüber böswilligen Attacken und Manipulation zu sein. »Security in times of pandemics and major global events«, war das Motto des erstmals zweitägigen »International Digital Security Forum« (IDSF). Es wurde vom AIT Austrian Institute of Technology und der Außenwirtschaft Österreich der Wirtschaftskammer im Dezember 2020 und in Zusammenarbeit mit go-international, einer gemeinsamen Initiative des Bundesministeriums für Digitalisierung und Wirtschaftsstandort, veranstaltet und fand coronabedingt als hybrides Onlineevent statt. Über den Dächern Wiens im 4. Bezirk wurden den Wissenstransfer und Kooperationen zwischen Forschung, Unternehmen, Verwaltung und Politik angestoßen. Das Interesse,



Vladimir Voronkov, Under-Secretary-General United Nations Office of Counter Terrorism in New York: »Globale Bedrohungen erfordern eine multilaterale Zusammenarbeit«.

Partnerschaften für die Bekämpfung und Schadensminimierung von Krisen zu bilden, war groß. An der Konferenz nahmen mehr als 500 Menschen aus über 40 Staaten teil.

>> Prominente Unterstützer <<

Eröffnet wurde das IDSF von Bundeskanzler Sebastian Kurz, der die Bedeutung von sicheren Lösungen in einer zunehmend digitalen und vernetzten Welt hervorhob, sowie von Wirtschaftsministerin Margarete Schramböck und Christian Weissenburger, Leiter der Sektion Innovation und Technologie im BMK in Vertretung von Bundesministerin Leonore Gewessler. Andreas Reichhardt, Sektionschef für Telekommunikation, Sicherheits- und Verteidigungsforschung im BMLRT, präsentierte in Vertretung von Bundesministerin Elisabeth Köstinger das österreichische Sicherheitsforschungsprogramm und verwies auf die hohe erreichte Qualität und Dynamik in der österreichischen Forschungs- und Entwicklungs-Szene. Innenminister Karl Nehammer betonte bei der Eröffnung des zweiten Konferenztages das hohe Interesse der Politik an dem Thema: »Wir wollen die digitale Welt zu einem erfreulichen und sicheren Ort machen: Unsere Anstrengungen heute sind lebenswichtig für eine prosperierende, sichere und demokratische digitale Zukunft.«

Die hohe Relevanz der im Rahmen der IDSF diskutierten Schwerpunkte wurde durch internationale Organisationen wie der UN begrüßt. Vladimir Voronkov, Under-Secretary-General des United Nations Office of Counter Terrorism (UNOCT) in New York, hob in seiner Rede die sich entwickelnden Bedrohungsszenarien hervor, die eine starke multilaterale Zusammenarbeit erfordern, um ihnen effektiv zu begegnen.

Arne Schönbohm, Präsident des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI) betonte in seiner Keynote wie wichtig es ist, die Hand zu allen internationalen Partnern auszustrecken und den Austausch mit allen relevanten Stakeholdern zu stärken; Europa sollte dabei viel selbstbewusster auftreten und die Entwicklung globaler Standards vorantreiben.

Schließlich erläuterte Vincent Waiswa Bagiire, Permanent Secretary at Ministry of Information Communications Technology and National Guidance von Uganda, die Wichtigkeit der Digitalisierung für ▶

HERAUSFORDERUNGEN FÜR KRYPTOWÄHRUNGEN

Kryptowährungen werden als vielversprechende Alternative zu traditionellen Finanzsystemen gehandelt. Die Schattenseite des Erfolgs ist der Missbrauch der digitalen Zahlungsmittel durch Kriminelle für Ransomware-Attacken, Geldwäsche und der Finanzierung von Terrorismus. Wie der Einsatz von Bitcoin und Co. dahingehend beobachtet und geschützt werden kann, sprach Bernhard Haslhofer, Thematic Coordinator Data Science, AIT, mit Eljo Haspels, CEO von Cointel, Niederlande, Haaroon Yousaf und George Kappos von der University College London, Univ. Prof. Rainer Böhme, Universität Innsbruck, und Kamal Anwar, UN-Office of Counterterrorism, New York. Der gemeinsame Tenor: Nur mit einer stärkeren internationalen Zusammenarbeit und mit dem Austausch von Know-how und Daten kann der Gebrauch von Kryptowährungen sicherer werden. Der Grund, warum internationale Terrororganisationen recht früh auf dezentral organisierte Währungen gesetzt haben, ist das Bedürfnis, außerhalb staatlich kontrollierter Systeme zu agieren. Die »helle Seite« kann dem mit neuen Analysemethoden und datenbasierter Forschung gegensteuern. Es ist freilich stets ein technologischer Wettlauf.

AIT-Forscher Bernhard Haslhofer diskutierte mit seinen Gästen, wie der Missbrauch von Kryptowährungen eingeschränkt werden kann.

Fotos: Valerie Maltseva/Agenda Studio

FAKE NEWS UNTERMINIEREN DEMOKRATIEN

Ross King, Head of Competence Unit Data Science & AI, AIT, diskutierte mit VertreterInnen der Zivilgesellschaft und ForscherInnen zur wachsenden Bedrohung durch Fake News. Dominika Hajdu und Miroslava Sawiris vom Thinktank GLOBSEC in Bratislava lieferten Zahlen aus einer MIT-Studie und eigenen Untersuchungen: Fake News verbreiten sich aufgrund ihrer oft emotionalen Inhalte schneller als reguläre Nachrichten. Und fast jeder zweite zentral- und osteuropäischer Bürger – abhängig von den persönlichen und wirtschaftlichen Perspektiven – glaubt nicht an die Ideale der Demokratie. Zwei Drittel halten aktuelle Covid-Maßnahmen für übertrieben oder überhaupt nicht notwendig. Caroline Schmidt, Innenministerium, wies auf Aktivitäten der österreichischen Regierung hin – eine »Austrian Disinformation Taskforce«, die bei Wahlen aktiv ist, oder das Projekt »Detection of false information by Artificial Intelligence«. Die EU nimmt sich des Themas Fake News mit einem »Action Plan against Disinformation« an. Laura Loguercio, Journalistin der Faktencheck-Website Pagella Politica, betonte die Notwendigkeit internationaler Zusammenarbeit im Kampf gegen Desinformation. Plattformen wie »SOMA Observatory« und »CoronavirusFactsAlliance« würden die Kooperation über Landesgrenzen hinaus unterstützen.

Ross King, AIT: »Die Menschen brauchen Tools, um Fake News und Desinformation erkennen zu können.«

KNOW-HOW FÜR KUNDEN WELTWEIT

Das AIT führte vom 16. bis 20. November 2020 im Auftrag der US Defense Threat Reduction Agency (DTRA) und der URS Federal Services International ein spezielles Cybersicherheitstraining für den sicheren Betrieb von Atomkraftwerken im Ausbildungszentrum für nukleare Sicherheit (NSTC) in Almaty, Kasachstan durch. Durch die aktuelle Covid-Situation wurde von AIT das gesamte Training virtuell durchgeführt. Das Ziel war es, sowohl Bewusstsein als auch Fähigkeiten zur Entwicklung, Implementierung und Aufrechterhaltung eines Informations- und Cybersicherheitsprogramms in einer kritischen Einrichtung zu entwickeln.

Kanzler Sebastian Kurz hob die Bedeutung von sicheren Lösungen in einer vernetzten Welt hervor.

BSI-Präsident Arne Schönbohm: »Europa muss selbstbewusster auftreten und die Entwicklung globaler Standards vorantreiben.«

▶ die soziale und wirtschaftliche Entwicklung afrikanischer Länder am Beispiel von Uganda, das bis 2040 den Wandel von einem Agrarland zu einem digitalen Staat schaffen will. Cybersecurity und internationale Kooperation sind dabei eine zentrale Grundlage.

>> Cybercrime, virtuelle Währungen und Fake News <<

Im Rahmen von zahlreichen Paneldiskussionen wurden Schlüsselthemen zur digitalen Sicherheit diskutiert: Cybersicherheit und Cybercrime, sichere Künstliche Intelligenz, Schutz vor Missbrauch von virtuellen Währungen, effektive digitale Plattformen für das Krisen- und Katastrophenmanagement, kontaktlose biometrische Sensortechnologien, Kampf gegen internationalen Terrorismus, sowie Resilienz von digitalen Infrastrukturen.

Ein besonderer Schwerpunkt lag auf dem Themenfeld »Kampf gegen Desinformation«, das durch die Corona-Krise noch brisanter geworden ist: Im Fokus standen dabei die Bedeutung von Fake News für die gesellschaftliche und politische Ordnung sowie die neue Rolle von Medien.

>> Europa soll Vorreiter sein <<

Für die Bekämpfung von Cyber-Kriminalität ist eine intensive internationale Zusammenarbeit nötig. »Kein Akteur auf der Welt kann derzeit alleine alle Herausforderungen abdecken. Wir müssen kooperieren, wie brauchen dafür Mechanismen, internationale Standards und Abkommen sowie ein gemeinsames Verständnis zur sicheren Verwendung des Internets auf unserem Globus«, sagte Helmut Leopold, Initiator der IDSF sowie Head of Center for Digital Safety & Security am AIT.

Mariana Kühnel, Generalsekretär-Stellvertreterin der Wirtschaftskammer Österreich und Co-Organisator der IDSF unterstrich: »Es ist unbestritten, dass das Coronavirus eine der größten Weltwirtschaftskrise ausgelöst hat, und noch weitere unvorhersehbare Folgen mit sich bringen wird. Durch diese Krise hat aber auch die Digitalisierung zugenommen. Das birgt für Unternehmen neue Chancen, aber auch Herausforderungen, etwa in Form von Cyberangriffen oder Datenlecks. Und bei digitaler Sicherheit geht es nicht nur um die Technologien, sondern um jeden einzelnen von uns. Der Faktor Mensch ist immer noch am angreifbarsten, und das muss allen in unserer neuen Welt bewusst sein. Ein interdisziplinärer und internationaler Austausch zu diesen Themen ist sehr wichtig.«

Europa komme dabei eine besondere Rolle zu, betonte Arne Schönbohm, Präsident des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI): «Wir haben in den EU-Staaten viel Expertise und Erfahrung. Es ist wichtig, dass wir uns mit diesen Ressourcen gegenseitig unterstützen und dass wir voneinander lernen«, sagte er. Die Initiativen der EU, wie etwa der Cyber Security Act aus dem Jahr 2019, würden auch die Partner in Asien und in Nordamerika beeinflussen. »Wir sollten selbstbewusster für eine weltweite Standardisierung in diesem Bereich auftreten«, so der Experte.

>> Kanus im Ozean <<

Dass viele IT-Systeme in der Praxis nicht gut genug vor Cyberangriffen geschützt sind, bestätigte Rafal Jaczynski, CSO bei Huawei CEE & Nordics. »Viele Unternehmen sind in den Digitalisierungs-Ozean mit Cybersecurity-Kanus gestartet«, sagte Jaczynski. Er betont, dass man zwar genügend Wissen und Technologie für sichere Systeme habe, aber viele Unternehmen und Organisationen der Sicherheit nicht genug Aufmerksamkeit schenken.

Zusätzlich zur Anwendung vorhandener Technologien müsse die Forschung verstärkt und die Überführung von Forschungsergebnissen in die Praxis beschleunigt werden, forderte Kai Rannenberg, Professor an der Universität Frankfurt und Koordinator des europaweiten Kompetenz-Netzwerks CyberSec4Europe. »Wir müssen uns ständig neue Kompetenzen aneignen, denn viel Wissen befindet sich auch in den Händen der Cyberkriminellen«, sprach sich Rannenberg für verstärkte internationale Zusammenarbeit aus. ■

»NEXT GENERERATION BORDER MANAGEMENT«

> Praktiker, Wissenschaftler, Vertreter der Industrie und der Regulierung sprachen mit Andreas Kriechbaum-Zabini, Thematic Coordinator Surveillance & Protection, AIT, über die Sicherheit an den Landesgrenzen der EU. Kontrollmechanismen bedeuten stets ein Ringen zwischen der Bewegungsfreiheit von Menschen und Güter und Maßnahmen gegen Bedrohungen in der physischen und digitalen Welt gleichermaßen ist. Es diskutierten unter anderen Giulio M. Mancini, Generaldirektion Migration und Inneres, EU-Kommission, und Romain Nivelle, Leiter der EU-Mission für die Region Hauts-de-France, in der auch der Hafen von Calais liegt. 10.000 Lkw-Fahrten täglich werden dort abgewickelt. Für ein automatisiertes und effizientes Grenzmanagement von Fahrzeugen und Menschen sorgt das Projekt FASTPASS unter der Leitung des AIT. James Ferryman von der Universität Reading, UK, fordert zukunftsfähige Konzepte für die steigenden Anforderungen an Mobilität und Sicherheit. Technologie – etwa am Smartphone oder auch mit elektronischen Pässen – könne auch zugunsten Reisender eingesetzt werden liefern, wenn dadurch Kontrollen rascher ablaufen und gleichzeitig Sicherheitschecks verbessert werden. Nötig dafür ist in der EU eine gemeinsame Sichtweise und Kooperation der Behörden und Beteiligten entlang der gesamten »Wertschöpfungskette« im Grenzverkehr.

Made in Austria: Andreas Kriechbaum-Zabini leitet internationale Projekte für die Grenzsicherheit.

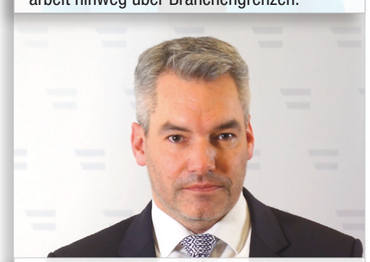
MIT BIOMETRIE GEGEN TERRORISMUS

> Über technologische neue Möglichkeiten zur Feststellung der Identität von Personen wurde in einer Gesprächsrunde von Bernhard Strobl, Thematic Coordinator Surveillance & Protection, AIT, berichtet. Gerade Corona und die notwendigen Gesichtsmasken sind eine neue Hürde für eine effiziente Personenerkennung. Reinhard Schmid, Leiter des zentralen Erkennungsdienstes des Bundeskriminalamtes, referierte zu EU-Recht, dem »Article 20 IO Interoperability Regulations« und das Pilotprojekt »BioCapture«, mit dem künftig die Exekutive mit dem Smartphone Fingerabdrücke zur Identifizierung von Personen nehmen kann – effizient und ohne weitere Technik. Rocco Messina und Margherita Natali vom United Nations Counter-Terrorism Centre (UNCCT), USA, diskutierten die verantwortungsvolle und angemessene Weitergabe von biometrischen Daten im Zuge der Terrorabwehr. Werkzeuge und Prozesse dazu sollten immer auch »human rights by design« beinhalten. Für Andreas Wolf, Principal Scientist Biometrics der deutschen Bundesdruckerei, werden erfolgreiche Projekte von drei Säulen getragen: Interoperabilität, Authentizität und Qualität. Als großen Trend machte die Runde – darunter auch IBM-Technologieexperte Nelson Goncalves – berührungslose Erfassungstechnologien aus, sowie Plattformen, die über Systeme und Behörden hinweg Daten analysieren können.

Bernhard Strobl, AIT: »Die Corona-Pandemie hat völlig neue Herausforderungen für biometrische Erkennungstechnologien in Europa gebracht.«

BMLRT-Sektionschef Andreas Reichhardt präsentierte das österreichische Sicherheitsforschungsprogramm und verwies auf breite F&E-Aktivitäten.

Wirtschaftsministerin Margarete Schramböck betonte die Tradition der Zusammenarbeit hinweg über Branchengrenzen.



Innenminister Karl Nehammer: »Anstrengungen für eine prosperierende, sichere und demokratische Zukunft.«

Fotos: Valerie Maltseva/Agenda Studio

Partnerschaften auf globaler Basis

> **Begleitet wurde das** IDSF von einer virtuellen Ausstellung österreichischer und internationaler Organisationen und Unternehmen wie ARGE Sicherheit und Wirtschaft der Wirtschaftskammer Österreich, ARES – Cyber Intelligence, Attingo Datenrettung, Cybertrap Software, Digital Factory der FH Vorarlberg, Huemer-IT, Ikarus Security Software, KIVU Technologies, Kuratorium Sicheres Österreich, Lieber Lieber Software, msg Plaut, SBA Research, Softprom Distribution, Sparx Systems Central Europe, T3K-Forensics, World Institute for Nuclear Security (WINS) sowie X-Net Services. Die Veranstaltung wurde unterstützt von Huawei, SAS Institute und T3K-Forensics.

> **Die Panel-Diskussionen sind** zur Nachschau auf der IDSF-Website für registrierte User unter www.idsf.io zur Verfügung gestellt.