Sicherheitskonferenz Krems: Walter Unger, Bundesheer; Johann Paul Brunner, Bezirksstellenleiter Krems des Roten Kreuzes a. D.; Günter Stöger, Bezirkshauptmann Krems; Maresa Meissl, Europäische Kommission, Peter Gridling, Direktor BVT a. D.; Bundesrätin Doris Berger-Grabner; Karl Wilfing, NÖ Landtagspräsident; Ingeborg Zeller, UWK; Rudolf Striedinger, Generalstabschef des Bundesheeres; Walter Seböck, UWK; Claudia Brandkamp, Deutsche Telekom; Peter Parycek, UWK

Neue Bedrohungsbilder

Unter dem Titel „A new world disorder? Perspektivische Sicherheitsbetrachtung nach 20 Jahren Sicherheitskonferenz“ fand am 19. Oktober 2022 in Krems die diesjährige Sicherheitskonferenz der Universität für Weiterbildung Krems in Kooperation mit dem Bundesministerium für Inneres statt.

Etwa 90 Expertinnen und Experten sowie Zuhörer aus Deutschland, Österreich und der Schweiz tauschten sich am 19. Oktober 2022 bei der Sicherheitskonferenz an der Universität für Weiterbildung Krems (UWK) aus. Einlader war das Team des Zentrums für Infrastrukturelle Sicherheit unter Federführung von Mag. Dr. Ingeborg Zeller. Im Zentrum standen das zwanzigjährige Jubiläum der Konferenz. Die Begrüßung erfolgte durch Vizerektor für Lehre/Wissenschaftliche Weiterbildung und digitale Transformation, Univ.-Prof. Mag. Dr. Peter Parycek, den Leiter des Zentrums für Infrastrukturelle Sicherheit, Ass.-Prof. Mag. Dr. Walter Seböck, den Präsidenten des Niederösterreichischen Landtages, Mag. Karl Wilfing, sowie dem Generalstabschef des Bundesheeres, General Mag. Rudolf Striedinger.

Gültigkeit und Aktualität. Der Titel „A new world disorder?“ erzeugt selbst nach 20 Jahren eine Gültigkeit, die aktueller nicht sein könnte – insbesondere, wenn es um Sicherheit geht. Angefangen von globalisierten Wirtschaftsformen über ständig neue Entwicklungs- und Schwerpunktverlagerungen bis hin zu der Frage, ob Demokratie und Gesellschaft, wie wir sie kennen, in Gefahr sind. Eines steht nach Seböck fest: Jeder Dialog schafft mehr Klarheit. Die Mission der kürzlich umbenannten Donau-Universität Krems (DUK) in Universität für Weiterbildung Krems (UWK) besteht in der Weiterbildung. Seböck betonte die essenzielle Kooperation zwischen Wissenschaft, öffentlicher Verwaltung und Wirtschaft, die eine erhebliche Rolle bei der Weiterentwicklung spielt.

Zeitreise. Vizerektor Parycek bekräftigte den Aspekt der Weiterbildung und ging auf eine Zeitreisedebatte der digitalen Souveränität ein. Dabei spannte er einen Bogen von Unsicherheiten hin zu einer positiven Aufbruchsstimmung, denn heute jage eine Krise die andere, aber digitale Souveränität sei keine national gedachte Frage, sondern eine europäische und globale. Eine österreichische Autarkie sei nicht möglich, aber das Anstreben von zumindest wechselseitigen Abhängigkeiten bleibt Ziel. Etwa Kompetenzen von vorhandenen Technologien in Anwendungen zu implementieren, wobei gleichzeitig ein Mindestmaß an Resilienz beizubehalten, systematische Schwachstellen zu identifizieren und eine europaweite Autarkie anzustreben sind. Im Wettbewerb zwischen den Vereinigten Staaten von Amerika und China, die sich auf diversen Ebenen absichern, wird Europa nirgends erwähnt. Darüber hinaus wurde die digitale Arbeitswelt und Handlungskultur von Parycek angesprochen, wobei gegenwärtige Wasserfall-Modelle – lineare Vorgehensmodelle im Projektmanagement – den Nachteil von langen Pro-

FOTO: ANDREA REISCHER

zessen aufweisen. Andere Formen von Ausschreibungen wären in diesem Bereich angedacht, um z. B. die Geschwindigkeit im Sicherheitsbereich voranzutreiben.

Menschengerechte Lösungen. Mag. Karl Wilfing, Präsident des Niederösterreichischen Landtages, in Vertretung von Landeshauptfrau Mag. Johanna Mikl-Leitner, ging auf die Transformation sowie eine damit im Zusammenhang stehende Erlangung menschengerechter Lösungen ein. Er sei zuversichtlich, dass die Menschheit trotz Krisen wie der Covid-19-Pandemie, dem Klimawandel sowie dem gegenwärtigen Krieg zwischen Russland und Ukraine, zuversichtlich bleibt. Man finde zwar nicht alle Antworten auf die Frage einer „new world disorder", allerdings könne man sich auf Eventualitäten wie ein Blackout vorbereiten.

Auf militärische Aspekte mit Bedrohungspotenzial ging General Mag. Rudolf Striedinger ein. Jenes im Osten sei sehr groß und betreffe alle weltweit. Durch seine Beschäftigung mit der strategischen Vorausschau anhand eines Rückblicks auf Ereignisse, lautete sein Fazit: Das Um und Auf liege in der Vorbereitung. Das Bundesheer diene als strategische Reserve der Republik, was stets unter Beweis gestellt wurde, z. B. in Einsätzen bei Naturkatastrophen oder der Covid-19-Pandemie. Auch hybride Bedrohungen gehören zum Tagesthema, allerdings „ist gegenseitiges Lernen das, was uns alle weiterbringt."

Politik für Menschen. Mag. Dr. Maresa Meissl, Leiterin des Referats Informationssicherheit in der Direktion Sicherheit der Europäischen Kommission, gab eine Rückschau auf die Entwicklungen in ihrem Bereich in den vergangenen zwei Jahrzehnten. Meissl ist für Aktivitäten im Zusammenhang mit Informationssicherheit einschließlich der Reaktion auf Cyber-Angriffe und der Personalakkreditierung zuständig.

Beginnend mit den Anschlägen auf die Twin-Towers 2001 in New York, wozu es acht Online-Beiträge zu IT-Sicherheit im deutschen Sprachraum gab, ist eine eindeutige Weiterentwicklung wahrzunehmen – heutzutage ist die Thematik wesentlich verbreiteter und es gibt zahlreiche deutschsprachige Beiträge in Online-Medien dazu. Mit dem Platzen der Internetblase war der Wettlauf Europas gegen die Vereinigten Staaten von Amerika bereits verloren geglaubt, allerdings stieg seitdem auch hier das Bewusstsein, dass etwas getan werden muss.

Der Weg für den Einstieg in die Cyber-Sicherheit wurde durch die NIS-Richtlinie (Netz- und Informationssystemsicherheit) im Jahr 2016 geebnet und befindet sich gegenwärtig in der Umsetzungsphase als NIS 2. Ziel ist es, Cyber-Sicherheit EU-weit zu verbessern. Die neuen Regelungen betreffen das Risikomanagement und die Ausweitung auf Unternehmen.

„Österreich weiß sich als kleines Land durchaus gut zu positionieren", sagte Meissl. Weitere dahingehende Bestrebungen liegen im AI-Act (Artificial Intelligence), dem Digital Service Act (DSA) sowie dem Digital Markets Act (DMA) der EU. Das positive Ergebnis im Jahrzehntevergleich liegt insbesondere darin, dass die Botschaft der Wichtigkeit dieser Bestrebungen sowohl bei den Entscheidungsträgern als auch bei den Menschen mittlerweile angekommen ist. „Wir müssen daran weiterarbeiten, denn Politik ist zwecklos, wenn sie nicht bei den Menschen ankommt."

Worms & Breaches. Über die Adaption von Cyber-Risiken klärte Ing. Thomas Mandl, Cyber-Defense Consulting Experte, auf. Mandl ist seit 1988 in der Technik- und IT-Branche tätig, zuletzt viele Jahre als CTO bei der IKARUS Security Software – dem einzigen österreichischen Hersteller und Know-how-Träger für Antivirus-Lösungen. Ausgehend vom sogenannten „morris worm", der sich selbstständig als Malware in den späten 1980er-Jahren rasant im Internet verbreitete, über den „I love you"-Virus im Jahr 2000 oder der „WannaCry"-Attacke im Mai 2017, der verheerende Auswirkungen bei den Gesundheitseinrichtungen in Großbritannien verursacht hat, war einiges an Cyber-Angriffen erfasst. Sein Angebot: „Wir haben Möglichkeiten, uns dagegen zu schützen." Durch Best Practices, also die besten derzeit bestehenden Modelle, wie man mit Angriffen in der Praxis umgeht, entsprechende Rahmenpläne könne man sich gut vorbereiten, um mit solcher Art von Attacken umzugehen. Mandl stellte die Frage, ob wir generell verlernt hätten, Risiken zu erkennen und ernst zu nehmen. Dabei führte er ein Beispiel von einer Person an, die während des Radfahrens versuchte, ein Selfie aufzunehmen. Dabei traf sein Hinweis, Vorschläge und Empfehlungen annehmen zu müssen, genau ins Schwarze. Denn die Cyber-Bedrohungslage kann in den nächsten Jahren noch deutlich zunehmen, weil man damit einfach Geld verdienen kann. Daher sollte man das Mindset in Richtung assume breaches stellen und dahingehend Zeit und Geld investieren – man sollte nicht von komplett angriffsresistenten Einrichtungen ausgehen, sondern sich auf mögliche Angriffe vorbereiten, also sie antizipieren.

Seine Top 5-Empfehlungen: Schulungen und interne „helping hands" etablieren, Risiko Management einführen sowie Notfallvorsorge, Business Continuity Management und Security Audits durchführen und das Pareto Prinzip anwenden – also best practices umsetzen.

Faktor Mensch und Gesellschaft. Die anschließende Podiumsdiskussion, unter Moderation von Florian Petautschnig, BA, ORF-Wissenschaftsredakteur, hatte das Thema „Disorder – Unordnung in der Sicherheit. Was bedeutet dies für den Faktor Mensch und die Gesellschaft?". Als Gäste waren Mag. David Blum, Stellvertretender Direktor Staatsschutz und Nachrichtendienst, Mag. Walter Unger, Oberst des Generalstabsdienstes des Bundesheeres, Dr. Claudia Brandkamp, Deutsche Telekom Security GmbH in Bonn, Tobias Wolf, Group Threat and Incident Manager der Swiss Re Group sowie Dipl.-Ing. Mag. Andreas Tomek, KPMG, geladen. Themen wie spontane Krisen sowie damit einhergehende Reaktionen, Herausforderungen und Pläne oder Menschen in kritischen Funktionen und wie sie dabei unterstützt werden können, wurden ausführlich diskutiert. Das rechtzeitige Hinschauen in der Gesellschaft sei gerade im Hinblick auf Prävention hilfreich, vor allem in Zeiten von Krisen.

Die 21. Sicherheitskonferenz Krems ist bereits in Planung und wird am 18. Oktober 2023 stattfinden. Weitere Informationen dazu finden sich unter: *www.donau-uni.ac.at/sicherheitskonferenz.* *Nicole Felicitas Antal*