Wien positioniert sich mit Cyber Security Week zum globalen Zentrum für Netzsicherheit

Hochkarätig besetzte Konferenz zum Schutz kritischer Infrastrukturen in der Landesverteidigungsakademie – wichtige internationale Akteure folgen Ruf nach Wien

Wien (OTS) – Am Donnerstag, 16.2.2017 markierte die internationale Konferenz „Cyberspace, Energy & Development – Protecting Critical Energy Infrastructure“ den Startpunkt eines laufenden Dialogs internationaler Player rund um die Sicherheit unserer kritischen digitalen Infrastrukturen. Als der Teil der „Vienna Cyber Security Week“ wurde die Konferenz von der Energypact Foundation in Kooperation mit Bundesministerium für Europa, Integration und Äußeres (BMEIA), dem Bundesministerium für Landesverteidigung und Sport (BMLVS), der Cybersicherheit Plattform der österreichischen Bundesregierung (CSP), sowie AIT Austrian Institute of Technology als wissenschaftlichem Partner und mit Unterstützung internationaler Organisationen wie der ITU (International Telecommunication Union), der IEC (International Electrotechnical Commission) oder dem UNODC (United Nations Office on Drugs and Crime sowie mit Partnern aus der Privatwirtschaft wie Ernst & Young organisiert. Internationale Experten aus dem staatlichen und privatwirtschaftlichen Bereich aus zwei Dutzend Ländern wie auch von internationalen Organisationen diskutierten Herausforderungen, Chancen sowie die Notwendigkeit der globalen Zusammenarbeit, die sich durch die Digitalisierung kritischer Infrastrukturen ergeben.

„Die Kriege der Zukunft werden nicht durch die Zahl der verfügbaren Panzer oder Bomber entschieden werden, sondern durch die Zahl der verfügbaren Cyber-Experten“, unterstrich der Sicherheitspolitische Direktor des Außenministeriums, Dr. Gerhard Jandl, die steigende Bedeutung des Cyber-Raumes für die nationale und internationale Sicherheit. Vor allem durch Angriffe auf die „kritische Infrastruktur“ kann das ganze öffentliche Leben lahmgelegt und ein Land in die Knie gezwungen werden, ohne dass ein einziger Schuss fällt. Zwar gab es bisher derart massive Angriffe noch nicht, aber angesichts der schon erfolgten Attacken auf Bankensysteme, Industrieanlagen, Militärinfrastruktur, Kommunikationseinrichtungen, etc. sei die Frage nicht mehr, ob so etwas geschehen werde, sondern nur noch die Frage, wann. Jandl riss einige mit der Abwehr solcher Angriffe bzw. mit Vergeltungsmaßnahmen verbundene, derzeit noch nicht gelöste Probleme an: die Frage der zweifelsfreien Zurechnung der Attacken zum wirklichen Verursacher, jene der Verhältnismäßigkeit der Antwort („echte“ Waffen zur Verteidigung gegen Cyber-Attacken?), jene der Geltung des Völkerrechts, insbesondere des Humanitätsrechts, im Fall eines „Cyber-Kriegs“, u.v.a.m. Angesichts jüngster Presseberichte über die Beeinflussung der öffentlichen Debatten und damit der Wahlergebnisse durch Cyber-Maßnahmen von außen stellte Jandl die Frage, ob nicht auch die öffentliche Meinungsbildung in gewisser Weise zur schützenswerten „kritischen Infrastruktur“ eines Landes gerechnet werden sollte.

Generalmajor Dr. Johann Frank, Leiter Direktion für Sicherheitspolitik, BMLVS: „Im Rahmen der „Vienna Cyber Security Week“ wurde österreichischen Cyberexperten die Möglichkeit gegeben vor UN- und OSZE Botschaftern, Verteidigungsattachés und OSZE Militärberatern sowie internationalen Cyber Experten, die österreichische Cybersicherheitsstrategie, das Programm zum Schutz kritischer Infrastrukturen sowie Ansätze des gesamtstaatlichen Cyberkrisenmanagements und die darin verhaftete Rolle des Österreichischen Bundesheeres, zu präsentieren. Das Bundesministerium für Landesverteidigung ist beim Thema „Schutz kritischer Infrastrukturen vor Cyberangriffen“ doppelt gefordert. Einerseits verfügt das Österreichische Bundesheer selbst über kritische Infrastrukturen, die es zu schützen gilt. Andererseits wird bei einem größeren Cyber Störfall vom Bundesheer eine Unterstützung im Rahmen des gesamtstaatlichen Cyberkrisenmanagements erwartet, beziehungsweise im „Worst Case“, im „Cyber Defence Fall“, dem Militär die Führungsrolle übertragen. Da Cyberangriffe auf kritische Infrastrukturen vor Staatsgrenzen keinen „Halt“ machen, erfordern solche Angriffe auch den Austausch und die Zusammenarbeit auf internationaler Ebene. Die Energypact Foundation als Veranstalter der „Vienna Cyber Security Week“ hat diesen Bereich als Handlungsfeld erkannt und bietet internationalen Akteuren sowie Cyberexperten eine Plattform, um sich über dieses Thema auszutauschen und den Anstoß für mögliche Kooperationen zu geben.“

Dr. Thomas Stubbings, Vorsitzender CSP: „Der internationale Multistakeholder-Dialog zum Thema Cybersicherheit und kritische Infrastrukturen in Wien zeigt die Bedeutung des Themas für die Gesellschaft, die Wirtschaft und die Verwaltung in Österreich. Die CSP als Public Private Partnership der österreichischen Bundesregierung mit den Betreibern kritischer Infrastrukturen hat dies von Anfang an unterstützt und aktiv mitgestaltet.“

Alexandre Dimitrijevic, Präsident der Energypact Foundation: „Wir wollen eine internationale technologie- und risikobewusste Gemeinschaft von Führungskräften, Forschern, Spezialisten und Stakeholdern aus allen Bereichen des Energiesektors schaffen, die bereit ist, im Zusammenhang mit dem national wie auch international immer größere Bedeutung einnehmenden Thema der Cybersicherheit gemeinsam an den Herausforderungen von heute und den Bedürfnissen von morgen zu arbeiten.“

Benjamin Weissmann, MBA, Geschäftsführer bei Ernst & Young und Leiter der Cyber Forensik Österreich: „Wie so oft in der Geschichte schafft die Menschheit Fakten, ohne sich über die Folgen im Klaren zu sein: die Digitalisierung hat still und heimlich nahezu alle unsere Lebensbereiche eingenommen, bis hin zu der kritischen, lebenserhaltenden Infrastruktur unserer Gesellschaft. Im krassen Gegensatz dazu hat sich Wien höchst aktiv und im vollen Bewusstsein zu einem international proaktiven Schritt zur Verbesserung dieser Situation entschieden. Die internationale Multistakeholder Konferenz zum Schutz kritischer Infrastruktur ist ein starkes Lebenszeichen, Public Private Partnerships als gemeinsamen Ansatz zum Schutz unserer globalen digitalen Zukunft zu etablieren."

DI Helmut Leopold, Head of Center for Digital Safety & Security am AIT Austrian Institute of Technology: „Nur durch die intensive Kooperation und Zusammenarbeit zwischen privaten und öffentlichen Organisationen über alle Ländergrenzen hinweg können die unterschiedlichen Aspekte von Cyber Security, die nicht nur technischer, sondern auch gesellschaftlicher, rechtlicher und politischer Dimension sind, berücksichtigt werden."

Mit dieser richtungsweisenden Stakeholder-Konferenz konnte sich Österreich als High-Tech-Standort für Cyber Security erfolgreich auf dem internationalen Parkett positionieren und damit auch den Grundstein für eine permanente globale Initiative, die von Wien aus gesteuert werden soll, legen.

Rückfragehinweis:

Mag. (FH) Michael Mürling
Marketing and Communications
AIT Austrian Institute of Technology
Center for Digital Safety & Security
T +43 (0)50550-4126 | M +43 (0)664 2351747
michael.muerling@ait.ac.at | www.ait.ac.at