Fotos: BSH

Die Teilnehmenden des Bundesverbandes Sicherheitspolitik an Hochschulen treffen sich zum Seminar Wirtschaft & Sicherheit in Hamburg

Cyberangriffe und kritische Infrastruktur

Wie funktioniert ein Cyber-Angriff? Und wie schlimm ist ein solcher Angriff auf kritische Infrastruktur wirklich? Mit diesen und vielen weiteren Fragen im Kopf reisten die Teilnehmenden des vom Bundesverband Sicherheitspolitik an Hochschulen (BSH) veranstalteten siebten Seminars Wirtschaft & Sicherheit nach Hamburg.

Erste Antworten erhielten sie von Dr. Matthias Schulze von der Stiftung Wissenschaft und Politik (SWP). Er erläuterte den Begriff des Cyberangriffs und die Kosten-Nutzen-Abwägung von Staaten, einen solchen Angriff zu tätigen: „Ein Cyber-Angriff auf kritische Infrastrukturen eines anderen Landes ist nur in einer Krise oder kurz davor wahrscheinlich", sagte Schulze. Am Vormittag des zweiten Tages referierte Moritz von Gernet von der Vattenfall GmbH über die vernetzte Sicherheit in Unternehmen. Er betonte, dass selbst ein stark gesichertes Firmennetzwerk nutzlos werde, wenn Mitarbeiter ihre Passwörter auf Zetteln unter die Tastatur ihres Arbeitsplatzes klebten. Im Anschluss daran gab Stefan Schumacher vom Magdeburger Institut für Sicherheitsforschung einen Überblick über die Themen Industriespionage und Wirtschaftskriminalität. Hierbei beeindruckte er die Teilnehmenden nicht nur mit einer Darbietung seiner Hackingfähigkeiten, sondern ordnete auch Deutschlands Position im internationalen Umfeld ein: „Fehlende IT-Sicherheitskultur ist nicht nur ein deutsches Problem." Den Tagesabschluss bildete der Workshop von Marian Corbe von KPMG. Nach einem kurzen Input erarbeiteten sich die Teilnehmenden hierbei in einer spannenden Simulation die Anwendung des deutschen IT-Sicherheitsgesetzes.

Das Seminar Wirtschaft & Sicherheit enthielt viele spannende Aspekte

Geschärfte Wahrnehmung

Tag drei des Seminars begann mit einem Vortrag von Fregattenkapitän Professor Frank Reininghaus vom Institut für Friedensforschung und Sicherheitspolitik (IFSH) über Trinkwasser als kritische Infrastruktur. Anhand von historischen und aktuellen Beispielen erläuterte er die potenziell destabilisierende Wirkung eines solchen Angriffs auf Gesellschaften. Im Anschluss daran beleuchtete er in einem zweiten Vortrag ausführlich den Nutzen sowie die Bedrohung durch Drohnen. Nach einem Vortrag von Andreas Dondera von der Zentralen Anlaufstelle Cybercrime (ZAC) der Polizei Hamburg ermöglichte am Mittwochnachmittag Phillipe Lorenz von der Stiftung Neue Verantwortung (SNV) einen Einblick in KI-Unternehmen. Dabei ging er darauf ein, wann Unternehmen, die mit Künstlicher Intelligenz arbeiten, zu seinem Sicherheitsrisiko werden können.

Den dritten Tag beendete Sven Jovy von der RWTH Aachen, indem er die Teilnehmenden in die Möglichkeiten von Open Source Intelligence zur Bekämpfung von Desinformationen und Fake News einführte. Am Donnerstag verging der letzte Tag des Seminars wie im Flug: im Rahmen des Vortrages des Journalisten Hakan Tanriverdi begaben sich die Teilnehmenden auf die Spur mutmaßlich staatlich gesteuerter Hacker, wobei Tanriverdi den Zusammenhang zwischen der Intention eines Hackers und seinem Vorgehen beleuchtete.

Insgesamt waren es sehr spannende und lehrreiche vier Tage in der Hansestadt, die nicht zuletzt dank der hoch engagierten Teilnehmenden zu einem großen Erfolg wurden und die sicherlich für viele den Beginn einer geschärften Wahrnehmung von Cyber und kritischer Infrastruktur darstellten.

Sophie Witte