Bund Deutscher Kriminalbeamter

5. CyberSicherheitsForum BW

16.09.2023

2023 ist die IHK Region Stuttgart mit ihren Räumlichkeiten in Stuttgart Gastgeber.

Die Örtlichkeit

Veranstalter ist das Ministerium des Inneren, für Digitalisierung und Kommunen. Partner sind das Ministerium für Wirtschaft, Arbeit und Tourismus, die Cybersicherheitsagentur (CSBW), das Landeskriminalamt BW, das Landesamt für Verfassungsschutz BW und in diesem Jahr die IHK Region Stuttgart. 800 Anmeldungen lagen für die hybride Veranstaltung am 15.09.2023 vor, Landesvorsitzender Steffen Mayer war für den BDK BW vor Ort. Anwesend und mein Sitzpartner war zudem auch unser Sprecher IT, Cybercrime + Digitale Spuren, Daniel Belz.

Im Fokus steht die Cyberresilienz.

Innenminister Thomas Strobl (CDU) betont in seinem Grußwort, dass Cybercrime, Cybersabotage und Cyberspionage zu den größten Herausforderungen des Jahrzehnts gehören. BND-Präsident Dr. Bruno Kahl ergänzt diese drei Punkte dann später noch um das vierte Thema Desinformation.

CSBW, Polizei und Verfassungsschutz

Die Rede von Minister Strobl fokussiert an vielen Stellen die Arbeit der CSBW mit ihrer 24/7-Cyberhilfe, dem Lagezentrum, den Schulungen und Veranstaltungen und Sicherheitsanalysen. Er gibt zudem bekannt, dass Warnmeldungen in der Zukunft auch IHK und Firmen zugehen sollen – eigentlich nicht die Kernzielgruppe der CSBW. Wir hätten keinen Flickenteppich in Baden-Württemberg, Polizei und Verfassungsschutz ergänzten das Angebot, so Strobl. Für meinen persönlichen Geschmack ein etwas zu großes Loblied auf die noch recht neue CSBW und zu wenig Fokus auf die jahrzehntelangen Player in der Kriminalitätsbekämpfung und im Wirtschaftsschutz, LKA BW und LfV BW. Fakt ist, die CSBW wurde gegründet, mit Stellen und Finanzmittel bedacht, von denen wir in der Polizei im Verhältnis nur träumen können und nun ist dieser Player auf die Bühne getreten und wir müssen schauen, wie wir das operative und strategische Geschäft des Alltags gemeinsam bestreiten.

Grußwort der IHK

Thomas Conrady, u. a Präsident der IHK Hochrhein-Bodensee, fordert die Unternehmen auf, offener mit dem Thema Cyberangriffe auf die Wirtschaft umzugehen und sich auszutauschen. Man müsse sich damit befassen. Er hatte Lob für Bund und Länder im Gepäck, aber das Bewusstsein für die Wichtigkeit des Themas Cyberresilienz müsse weiter gestärkt werden.

Blick aus der Wissenschaft

Prof. Dr. Haya Shulman, mit einem Lehrstuhl an der Goethe-Universität in Frankfurt/Main, wagt den Blick in die Vergangenheit und die Zukunft im Bereich Malware. Was über die Jahre bleibt, ist der zumeist nur reaktive Ansatz auf Bedrohungen bzw. Schadenseintritte nach dem Tag x zu reagieren.

Prof. Shulmann weist darauf hin, dass die Durchlässigkeit zwischen Staat, Sicherheitsbehörden, Wirtschaft und Forschung in Israel sehr viel durchlässiger ist und dass dieser Schulterschluss zusammen mit der außenpolitischen Lage ein großer Motor für Innovation ist. Zudem sind die Leute stolz darauf beim Militär oder staatlichen Einrichtungen arbeiten zu dürfen. Denn auch sie weiß, dass in Deutschland beim Staat nicht alles über die Bezahlung zu regeln ist.

Polizeilicher Takedown von HIVE

Mit EKHK Daniel Lorch stellt dann das PP Ruutlingen (sic!) seine Mitarbeit im Takedown von HIVE dar. In der amerikanischen Pressekonferenz gelang die Aussprache „Reutlingen“ nicht ganz, aber völlig zurecht durfte man landesweit auf die Nennung in den Medien stolz sein. EKHK Loch wies darauf hin, dass weltweit alle 30 Sekunden ein schwerwiegender Cyberangriff erfolgreich durchgeführt wird und, dass die Arbeitsteilung in den internationalen Gruppierungen (Cybercrime as a Service) in den letzten Jahren einen wahren speed up erlebt hat. Insofern freue er sich auf die neue Zentralstelle bei er Justiz zur Bekämpfung der Cybercrime in Karlsruhe. Wir als BDK im Übrigen auch.

Blick in das Ausland - Bundesnachrichtendienstbericht

BND-Präsident Dr. Kahl legt den Fokus auf die Zuständigkeit seiner Behörde, die Bedrohungen im Ausland für deutsche Interessen und die Bedrohung aus dem Ausland mit Wirkung im Inland. Nach wie vor seien Russland und China die größte Bedrohung im Cyberraum. Dabei wären russische Gruppierungen häufig von Geldinteressen getrieben, mit wenig Sorge um Strafverfolgung im eigenen Land und die Gruppierungen aus der Volksrepublik China wären eher verbunden mit der Volksbefreiungsarmee oder nachrichtendienstlichen Behörden, also im Regelfall staatlich gelenkt. Ransomwareangriffe würden inzwischen auch dazu genutzt, die eigentlichen Ziele wie Datenexfiltration und die Vorbereitung von Sabotagehandlungen in der Zukunft zu verschleiern. Das macht es sowohl für die Dienste, als auch für die Polizei schwieriger.

Vernetzung, Transparenz, Investitionen

Alle Akteure sprachen von der Notwendigkeit der besseren Vernetzung, des Austausches und auch vom offenen Umgang mit Cybervorfällen, nicht zuletzt durch Anzeigenerstattung bei den Behörden. Das kann man nur unterstreichen.

Die Veranstaltung bot dann noch eine Podiumsdiskussion mit Frau Prof. Shulman, BND-Präsident Dr. Kahl und Innenminister Strobl und ging nach dem Mittag über in diverse Panelveranstaltungen mit den Schwerpunkten Resilienz, Krisenmanagement und Cybersicherheit sowie einem Panel „Live-Hacking“.

Eine gelungene Veranstaltung in ihrer fünften Ausgabe.

Apropos Nachbetrachtung

In einer Nachlese zwischen Daniel Belz und Steffen Mayer kamen wir auf einen Hinweis unseres Innenministers Thomas Strobl zu sprechen.

Er sagte: "Cybersicherheit kostet Geld, **keine** Cybersicherheit kostet noch viel mehr Geld".

Das stimmt! **Allerdings müssen diese Investitionen auch in die Polizei hinein erfolgen.** Das Katz-und-Maus-Spiel zwischen Räuber und Gendarm ist hier besonders nachteilig für den Gendarmen angelegt. Mit Blick auf die Landtagsdrucksache 17/5254 "Kampf gegen Cyberkriminalität in Baden-Württemberg" werden wir das nochmals an anderer Stelle näher ausführen.

Steffen Mayer, Landesvorsitzender BW

(Bildquelle: BDK BW, Daniel Belz)