AFCEA Bonn e.V.

Gemeinsam für mehr Sicherheit

AFCEA Bonn e.V. hat sich seit der Gründung 1983 der Zielsetzung verschrieben, seinen Mitgliedern und der interessierten Öffentlichkeit ein Spezialforum moderner Informations- und Kommunikationstechnologie zu bieten. Das Anwenderforum für Fernmeldetechnik, Computer, Elektronik und Automatisierung (AFCEA) Bonn e.V. umfasst als gemeinnütziger Verein ohne kommerzielle Interessen über 900 persönliche und mehr als 90 Firmenmitglieder und ist Teil des internationalen Netzwerks AFCEA International. Die persönlichen Mitglieder haben aufgrund ihres fachlichen Hintergrundes und ihrer Neigung zum Meinungsaustausch zu uns gefunden. Zu den Firmenmitgliedern gehören neben den Großen der IT- und Kommunikationsbranche eine Vielzahl mittelständischer und kleinerer Unternehmen vornehmlich aus der Region Bonn-Köln-Koblenz. Auch in Berlin und anderen Regionen Deutschland ist der Verein aktiv für den Wissensaustausch engagiert.

Innere und äußere Sicherheit 4.0 – Schlüssel zur „digitalen Souveränität“

Das Jahresthema lautet 2017 „Innere und äußere Sicherheit 4.0 – Schlüssel zur digitalen Souveränität“ gewählt. AFCEA Bonn e.V. möchte als gemeinnützige, unparteiische Organisation bei der Information unterstützen und auch kritischen Fragen wie vorhandenen Antworten Raum bieten. Expertise und eminente Fähigkeiten gibt es auf staatlicher und industrieller Seite durchaus – das akademische Potential in Deutschland kann sich sehen lassen.

Doch die Bedrohung wird immer sichtbarer: Die Beeinflussung des US-Wahlkampfes, Hackerangriffe auf Energieversorger und die NATO-Website, Cyberangriffe auf militärische Systeme oder der Fall Lisa. So mancher stellt sich die Frage: „Droht eine Situation wie vormals im Wilden Westen?“

Das Austesten der Resilienz unserer Gesellschaft, die Angriffe auf staatliche Organe und die Einsatzfähigkeit der Streitkräfte sind absehbar der Anfang. Eigentlich positive technologische Entwicklungen wie Big Data, ausgeklügelte Data Analytics, neue Formen der Automatisierung oder das Internet of Things bieten neue Anfälligkeiten für Manipulation und Störungen großer Datenmengen, ihrer Validität und Integrität. Zudem schreiten Entwicklungen heute so rasch voran, dass nur wenige Experten die fortlaufend verbesserten Techniken, Angriffsvektoren, Pläne von schwer zu enttarnenden Akteuren tief und rasch genug analysieren können.

„Für den eigenen Schutz gilt es, dem Gegner (möglichst) immer eine Nasenlänge voraus zu sein“, lautet die Devise. Das verlangt nach Kenntnissen, die einem Akteur zur Verfügung

P. Schartner · A. Baumann (Hrsg.) · D•A•CH Security 2017 · syssec (2017) 462-463.

stehen. Daher dürfen generell, neben dem Austausch auch nachrichtendienstlich erlangter Erkenntnisse, offensive Operationen im gegebenen rechtlichen Rahmen kein Tabu sein.

Keine der Abwehr- oder Präventionsmaßnahmen werden ohne die Akzeptanz und das Mitwirken der Bevölkerung greifen. Allmählich entwickelt sich in Deutschland ein entsprechendes Bewusstsein, ebenso die Erkenntnis, dass innere und äußere Sicherheit auf keinem Gebiet so eng verbunden sind wie im Cyber-Raum. Denn hierauf zielt letztlich jeder staatlich gelenkte Angriff aus dem Cyber-Raum ab: Auf die Entscheidungen des Bürgers als des Souveräns. Zugleich dürfte klar geworden sein: Deutschland braucht mehr, viel mehr junge Talente und am aktiven Schutz unserer Cyber-Souveränität Interessierte, als derzeit zur Verfügung stehen.

Gerade wenn es um Bewusstwerdung und Talentförderung geht, kann dies nicht eine Angelegenheit staatlicher Stellen alleine sein. Auch hier müssen sich staatliche, potente nicht-staatliche Akteure und freiwillige Unterstützer besser vernetzen. Das Verständnis, dass Cyber-Schutz, Cyber-Hygiene nicht nur eine staatliche Aufgabe ist, muss durch einen „whole-of-a-nation"-Ansatz bis hinein in die Ausbildungseinrichtungen getragen werden. Nicht von ungefähr nutzt Cyber viele Begriffe aus der Gesundheitsvorsorge (z.B. „Cyber-Hygiene"). Hackathons dürfen nicht länger den Ruf des Halbverbotenen haben, sie müssen als sportliche Erfahrung in den Dienst der Gemeinschaft gestellt werden. Dabei sollte die Nähe zu staatlichen Stellen (einschließlich der militärischen und Verfassungsschutzorgane) nicht pikiert gescheut, sondern als Beitrag zur Verteidigung der Bundesrepublik und unserer Lebensart verstanden werden. Warum nicht hier ein neues, positives Bild von Vorbildern bei Jugendlichen etablieren? Für die Immunisierung und Resilienz gegen Cyberangriffe sind viele, wahrscheinlich zu verknüpfende Wege und Mittel denkbar: Lernen aus Fehlern, hochentwickelte technische Abwehr, gesetzliche Verhaltensregeln, Folgen-Haftung bei grober Fahrlässigkeit. Das gilt für die gesellschaftliche wie die individuelle Ebene – jedes Individuum ist gefordert – wir alle müssen noch mehr tun!

AFCEA ist eine Plattform, um dies zu diskutieren und Wege in diese Richtung zu finden.

Kontakt

Jochen Reinhardt
Vorstand Medien
jochen.reinhardt@afcea.de

AFCEA Bonn e.V.
Borsigallee 2
53125 Bonn
T: 0228 925 82 52
F: 0228 925 82 53