Das Baltikum : Avantgarde der Cyber Defence

Autor(en): **Wegmüller, Hans**

Objekttyp: **Article**

Zeitschrift: **ASMZ : Sicherheit Schweiz : Allgemeine schweizerische Militärzeitschrift**

Band (Jahr): **178 (2012)**

Heft 6

PDF erstellt am: **23.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-309591

Das Baltikum – Avantgarde der Cyber Defence

Vor fünf Jahren wurde Estland Opfer eines massiven Cyber-Angriffs: Während dreier Wochen wurden die Server des Parlaments, der Ministerien, der Banken und Medien gestört oder gar lahmgelegt, was wie ein Fanal des Aufbruchs und der Sensibilisierung wirkte und im ganzen baltischen Raum zu einer beispielhaften Entwicklung im Bereich Cyber Defence führte.

Hans Wegmüller, Redaktor ASMZ

Das Thema Cyber Defence ist nicht neu, doch werden die Anforderungen in diesem Bedrohungsfeld durch den rasanten technologischen Fortschritt und die zunehmende internationale Vernetzung immer komplexer und anspruchsvoller. Die baltischen Staaten, allen voran Estland, scheinen seit jeher einen Hang zur Nische der Spitzentechnologie im IT-Bereich gehabt zu haben. So stammt zum Beispiel die Software zu Skype ursprünglich aus Estland, und man trug sich dort bereits im Jahre 2003 mit dem Gedanken, ein Kompetenzzentrum für Cyber Defence zu schaffen. Als Estland im Jahre 2007 Opfer eines der bisher massivsten Cyber-Attacken wurde, wirkte dies im ganzen baltischen Raum wie ein Fanal und führte zu einer erhöhten Sensibilisierung von Politik und Öffentlichkeit. So wurde der bereits seit Jahren vorliegende Plan zur Gründung eines Kompetenzzentrums für Cyber Defence im Mai 2008 umgesetzt: Mit Hilfe von «Sponsoring Nations», darunter die beiden andern baltischen Staaten Lettland und Litauen, wurde das «Cooperative Cyber Defence Centre of Excellence» (CCDCOE) mit Sitz in Tallinn ins Leben gerufen.

Das Kompetenzzentrum in Estland generiert Wissen und Erfahrungswerte im facettenreichen Bereich der Cyber Defence und ist eines von fünfzehn «Centres of Excellence» der NATO.

Das Zentrum in Tallinn ist heute eines von nunmehr insgesamt fünfzehn «Centres of Excellence» der NATO, die nicht Bestandteil der NATO-Kommandostruktur sind, jedoch durch das «Allied Command Transformation» akkreditiert werden, um offiziell von der NATO anerkannt zu werden. Das estnische Kompetenzzentrum generiert Wissen und Erfahrungswerte im facettenreichen Bereich der Cyber Defence. Dazu gehören Konzepte, Training, Planung und Durchführung von Übungen für NATO-Staaten, die Publikation von Forschungsergebnissen sowie juristische Unterstützung.

Seine Ausstrahlung reicht somit weit über die Landesgrenzen hinaus – im Juni dieses Jahres findet in Tallinn die «4th International Conference on Cyber Conflict» statt.

Cooperative Cyber Defence Centre of Excellence (CCDCOE) mit Flaggen der unterstützenden Nationen. Bilder: CCDCOE

Katalysator für den baltischen Raum

Der Technologie- und Sensibilisierungsschub, der durch die Ereignisse in Estland ausgelöst wurde, hat auch die übrigen baltischen Staaten beeinflusst und erfasst. Nicht nur gehören Lettland und Litauen zu den Gründernationen des estnischen Kompetenzzentrums, sondern sie entsenden seither auch eigene wissenschaftliche Vertreter nach Tallinn, und Lettland denkt zurzeit über einen weiteren Ausbau der Zusammenarbeit nach, wie der Chef der «Civil-Military Cooperation Section» im lettischen Verteidigungsministerium bestätigt. Die Führungsfunktion Estlands und die enge Zusammenarbeit wirken somit als Katalysator im baltischen Raum, was das Niveau im Bereich Cyber Defence in allen baltischen Staaten hochhält und stets neu befruchtet. Innovationen und Bewährtes werden übernommen, so plant etwa Lettland die Aufstellung einer speziellen Einheit für Cyber Defence in der Nationalgarde, einer Art Milizeinheit aus freiwilligen IT-Experten, wie sie in Estland seit

ungefähr zwei Jahren bereits besteht. Zudem wird gegenwärtig an einem «Memorandum of Understanding» im Bereich Cyber Defence gearbeitet, welches in Bälde in Kraft treten und die Zusammenarbeit zwischen allen drei baltischen Staaten noch intensiver und gezielter gestalten soll.

Beispiel Lettland

Lettland hat letztes Jahr seine Strategie der nationalen Sicherheit («National Security Concept») verabschiedet, welche sieben Teilbereiche umfasst, wobei ein Teil der IT-Sicherheit gewidmet ist. Somit ist Cyber Defence in Lettland – beispielhaft – integraler Bestandteil einer umfassenden nationalen Sicherheitsstrategie. Gleichzeitig wurde eine gesetzliche Grundlage geschaffen, das «Information Technologies Security Law», welches unter anderem nationale und lokale Behörden sowie private Firmen und Institutionen zur Kooperation verpflichtet und Aufgaben und Rechte des bereits erprobten Instrumentariums zur Umsetzung der Massnahmen im Bereich Cyber Defence umfassend auflistet und umschreibt.

«Ohne intensive internationale Kooperation wären wohl auch die baltischen Kleinstaaten nicht imstande gewesen, den heute beachtlichen Stand im Bereich der Cyber Defence zu erlangen.»

Im Unterschied zu Estland, wo für Cyber Defence grundsätzlich das Verteidigungsministerium verantwortlich zeichnet, wird in Lettland der «National IT Security Council» durch den Chef der Sicherheitsabteilung im Ministerium für Transport und Kommunikation präsidiert. Dieses Gremium ist zuständig für die Koordination der vom Gesetz vorgesehenen Zielsetzungen und Massnahmen. Ihm gehören ausserdem ein Vertreter der Streitkräfte (Vizepräsidium), des Aussenministeriums, des Ministeriums für Umweltschutz und regionale Entwicklung, der lettischen Nationalbank, Vertreter der Staatssicherheitsdienste und der «IT Security Incidents Response Institution» an. Letztere ist eine ständige Behörde, die ebenfalls unter der Aufsicht des Transport- und Kommunikations-Ministeriums steht, sehr eng mit dem Institut für Mathematik und Computer-Wissenschaften der Lettischen Universität in Riga liiert ist und im Ganzen aus 15 Vertretern relevanter Behörden und Institutionen besteht. Der «IT Security Incidents Response Institution» obliegt die ständige Überwachung («monitoring») der lettischen IT-Netzwerke, sie analysiert laufend Vorfälle wie Virenbefall, Diebstahl von Computern, «Denial of service»-Attacken etc., leitet Gegenmassnahmen ein, berät betroffene Behörden, Firmen, Institutionen und Einzelpersonen und zeichnet für die Planung und Durchführung von entsprechenden Übungen verantwortlich. Auch ihr Verhalten im Fall von routinemässigen Vorkommnissen im Bereich der IT-Sicherheit wird im Gesetz geregelt, wobei für den Krisenfall («in case of state emergency») eine Verstärkung durch Armeeangehörige vorgesehen ist. Periodisch werden von der «IT Security Incidents Response Institution» sogar «Tage der offenen Tür» organisiert, wo jedermann seinen Laptop mitbringen und ihn überprüfen und «reinigen» lassen kann.

In Lettland ist Cyber Defence – beispielhaft – integraler Bestandteil einer umfassenden nationalen Sicherheitsstrategie und das Land verfügt über ein erprobtes Instrumentarium im Bereich Cyber Defence.

Ausbildung im Cooperative Cyber Defence Centre of Excellence (CCDCOE).

Ohne intensive internationale Kooperation, Wissens- und Erfahrungsaustausch wären wohl auch die baltischen Kleinstaaten nicht imstande gewesen, den heute beachtlichen Stand im Bereich der Cyber Defence zu erlangen. Nach Aussage des Chefs der Abteilung Sicherheit im Transport- und Kommunikationsministerium arbeitet Lettland nicht nur sehr eng mit den baltischen Nachbarn, sondern auch mit der nordischen Staatenwelt (Finnland, Schweden, Norwegen, Dänemark), den einschlägigen EU- Gremien, insbesondere mit der Europäischen Agentur für Netz- und Informationssicherheit (ENISA), und der NATO zusammen.

Vergleich mit der Schweiz

Der Bundesrat beauftragte am 10. Dezember 2010 das VBS, bis anfangs 2012 eine gesamtheitliche Strategie des Bundes gegen die tendenziell steigenden Cyber Risiken zu erarbeiten. Was hierzulande mit Recht als notwendiger und richtiger Schritt in die Zukunft gerühmt wurde, haben die baltischen Staaten bereits seit längerer Zeit hinter sich. Die nunmehr in der Schweiz eingeleiteten Massnahmen im Bereich Cyber Defence erscheinen vor dem Hintergrund des aktuellen Standards in den baltischen Kleinstaaten eher als dringender und überfälliger Nachholbedarf denn als fortschrittliche Innovation. ■