Unseminar: Austoben auf dem digitalen Schlachtfeld

Strausberg/Berlin, 03.05.2016.

Das Zentrum Informationsarbeit Bundeswehr in Strausberg hat das erste Unseminar zum Thema Cyber- und Informationsraum veranstaltet. Vom 24. bis zum 27. April haben die Teilnehmer nicht nur einen innovativen Einblick in die sicherheitspolitischen Herausforderungen erhalten; sie konnten auch ihre eigenen strategischen Cyber-Fähigkeiten in einem Planspiel testen.

Ganz ohne Computer – nur auf Papier: Im Mini-Planspiel laufen die Köpfe heiß. (Quelle: Bundeswehr/Kellner)Größere Abbildung anzeigen

„Wir haben gewonnen“, schallt es selbstsicher aus der Ecke von Team Rot. Die drei Teammitglieder müssen selbst schmunzeln dabei, denn sie haben ihren Plan noch gar nicht vorgestellt und Gewinner oder Verlierer gibt es hier nicht. Rot steht für Angreifer. Sie sollen sich ein Szenario mit einer Cyber-Attacke ausdenken. Zur Verfügung stehen 15 Spezialisten, 15 Monate Zeit und mindestens 15 Millionen Euro. Rechtliche oder ethische Einschränkungen müssen nicht beachtet werden. Henning Hetzer hat schließlich das Motto ausgegeben: „Darüber nachdenken, was denkbar ist.“

Unblutiger Machtwechsel, Erhalt der Infrastruktur

Hetzer arbeitet im Referat Zukunftsanalyse im Planungsamt der Bundeswehr. Für das Unseminar hat er das Mini-Planspiel konzipiert, das die Teilnehmer im Verteidigungsministerium durchführen. Eine Stunde lang laufen die Köpfe heiß, um dann Ziele, Mittel, Effekte und den Schaden zu präsentieren. „State Owning – Der psycho-digitale Ansatz“, hat Team Rot die Attacke benannt. Politiker werden kompromittiert, Logistikzentralen der Nahrungsmittelindustrie lahmgelegt und als Krönung der Strom ausgeschaltet.

Engagiert präsentiert Rot diesen Plan am Flipchart: „Es wird das totale Chaos herrschen!“ Sie vertreten eine fremde Macht, die dann ihre Hilfe anbieten wird und über die Unterstützung inländischer Kräfte quasi die Herrschaft übernimmt. Es ist eine bis ins Detail durchdachte Kampagne, die zu einer hybriden Konfliktlage führt. Daten werden gestohlen, Systeme gehackt und Informationen manipuliert; die Herbeiführung eines unblutigen Machtwechsels bei Erhalt der Infrastruktur ist das Ziel.

„Es kann ein attraktiver Operationsraum sein, weil zunächst keine Schüsse fallen“, sagte Dr. Florian Schaurer zuvor dazu, warum Deutschland sich auch im Cyber-Raum schützen muss. Der Referent aus der Abteilung Politik im BMVg [Bundesministerium der Verteidigung] erklärte in einem Vortrag über die Herausforderungen der Verteidigungspolitik im Cyber- und Informationsraum, dass das Verteidigungsministerium eng mit dem Bundesinnenministerium in Sachen Cyber-Sicherheit kooperiere und hinsichtlich der völkerrechtlichen Fragen mit dem Auswärtigen Amt zusammenarbeite. Dr. Schaurer machte auch deutlich, dass für Einsätze im Cyber- und Informationsraum selbstverständlich der Parlamentsvorbehalt gelte.


Team Rot präsentiert den Angriffsplan. (Quelle: Bundeswehr/Kellner)Größere Abbildung anzeigen

Der Hacker macht den Einstieg

Team Rot muss sich nicht mit demokratischen oder rechtsstaatlichen Prinzipien auseinandersetzen. Sie müssen „böse Dinge tun“. So einfach hat Stefan Schumacher die Tätigkeit von Hackern, Kriminellen und Spionen im Netz beschrieben. Von Schumacher haben die roten Teams am Vortag gelernt, wie lange es dauern kann und was man können muss, um Netzwerke, Rechner oder Systeme zu infiltrieren und welche Software dafür notwendig ist.

Die Nerd-Sticker auf seinem Notebook erklären sofort, mit wem man es zu tun hat: Er sei „Geek, Nerd und Hacker seit mehr als 20 Jahren“, sagt Schumacher, der geschäftsführender Direktor des Magdeburger Instituts für Sicherheitsforschung ist. Auf seinem Notebook demonstriert er, wie schnell fremde Systeme infiltriert werden können. Kein Geheimnis: Die Software dazu kann im Internet heruntergeladen werden. Die große Herausforderung sei das Verschleiern des Angriffs; der Aufbau eines Botnetzes.

Team Rot hat dafür Spezialisten eingekauft. Doch welchen Schaden können sie anrichten? Damit muss sich Team Blau auseinandersetzen, die Verteidiger. Ihr Schwerpunkt sind die kritischen Infrastrukturen, auch KRITIS genannt. Team Blau bewertet nicht nur die Schadenshöhe, sondern auch die Eintrittswahrscheinlichkeit von Angriffen auf Atomkraftwerke, Strom- und Wasserversorgung, et cetera. Sie identifizieren eine entscheidende Sicherheitslücke in ihrem Risikomanagement: „Der Faktor Mensch ist unberechenbar.“

Das Mini-Planspiel mit der anschließenden Diskussion war einer der Höhepunkte im Unseminar „Von Nullen und Einsen – Sicherheitspolitische Herausforderungen im Cyber- und Informationsraum“. Die viertägige Veranstaltung bot den Teilnehmern darüber hinaus die Gelegenheit, unmittelbare und praktische Einblicke in die Arbeit von Institutionen und Behörden zu bekommen mit Exkursion, Expertenvorträgen und Podiumsdiskussion.


Unseminar: Unmittelbare Einblicke in die Arbeit von Institutionen und Behörden. (Quelle: Bundeswehr/Kellner)Größere Abbildung anzeigen

Entscheidungen treffen und kommunizieren

In der Seminarevaluation gab es auf der einen Seite den Wunsch, die Wirtschaft im Seminar stärker in den Fokus zu rücken. Für andere

war es jedoch genau der richtige Schwerpunkt: „Die Konzentration auf die staatliche Ebene war für mich besonders spannend“, sagte ein Selbstständiger aus der IT-Branche. „Das sind Fragestellungen, die mich beschäftigen, denn auch wir spielen Angriffsszenarien durch“, ergänzte er mit Blick auf das Mini-Planspiel. Die Unseminare richten sich an Führungskräfte aus Wissenschaft, Industrie, Gesellschaft und Politik. Vom Gymnasiallehrer über den echten Nerd bis zur Anti-Sabotage-Beauftragten eines Großunternehmens reichte das Spektrum der Teilnehmer.

Für den IT-Berater und Reserveoffizier René Schmiedgen lieferte das Unseminar „ganz wichtige Denkanstöße, die so nicht zu erwarten waren“. Insofern ist das Konzept der Unseminare – kurz, prägnant und ergebnisoffen sicherheitspolitische Themen zu vermitteln – aufgegangen. „Wichtig ist uns, dass die Seminarteilnehmer bei diesem offenen Seminarprogramm auch selbst Entscheidungen treffen und diese kommunizieren müssen“, sagt Oberstleutnant Alexander Willing vom Zentrum Informationsarbeit Bundeswehr.

„Vor dem Hintergrund der aktuellen Entwicklungen im Ministerium und der Bundeswehr könnte dieses Seminarthema einen festen Platz in unserer neuen Veranstaltungsreihe einnehmen“, so Willing. Denn zeitgleich zum Seminar hatte Verteidigungsministerin Ursula von der Leyen die Pläne zur Bündelung der Cyber- und IT-Fähigkeiten der Bundeswehr vorgestellt. Vorgesehen sind die Einrichtung einer eigenständigen Abteilung im BMVg [Bundesministerium der Verteidigung] und die Aufstellung eines militärischen Organisationsbereichs für den Cyber- und Informationsraum (CIR) mit einem Inspekteur an der Spitze sowie zwei neuen Dienststellen. Deutschland stellt sich auf die ernstzunehmende Bedrohung ein.

- **MEHR ZUM THEMA**

  - Das Unseminar – das offene Format
  - Dossier: Cyber-Verteidigung

- **WEITERE INFORMATIONEN**
  WEITERFÜHRENDE LINKS
  - Das Zentrum Informationsarbeit Bundeswehr im Internet

Stand vom: 06.05.16 | Autor: Florian Manthey
