Süddeutsche.de Digital

5. April 2017, 05:17 IT-Sicherheit

Die Bundeswehr rüstet sich für den Cyberkrieg

- Die Bundeswehr stellt sich für die Kriegsführung der Zukunft auf.
- Der neue Inspekteur Ludwig Leinhos sieht Cyberangriffe als attraktive Option.
- Kritiker warnen, dass die Bundeswehr zu einem internationalen Aufrüsten beitrage.

Von Christoph Hickmann und Hakan Tanriverdi

Ursula von der Leyen wird an diesem Mittwoch in Bonn erwartet. Für eine Verteidigungsministerin ist die ehemalige Bundeshauptstadt immer eine Reise wert, schließlich befindet sich dort, auf der Hardthöhe, nach wie vor der erste Dienstsitz des Hauses. Diesmal jedoch ist die Mission der Christdemokratin eine besondere.

"Bundesministerin der Verteidigung stellt neues Kommando Cyber- und Informationsraum auf", so ist die Pressemitteilung überschrieben. Von der Leyen, so geht es in typischer Bundeswehr-Diktion weiter, werde das Kommando "im Rahmen eines feierlichen Appells in Bonn in Dienst stellen und Generalleutnant Ludwig Leinhos zum ersten Inspekteur ernennen". Damit sei "ein weiterer Meilenstein erreicht, um die Bundeswehr künftig modern und innovativ gegen Bedrohungen aus dem Cyber- und Informationsraum aufzustellen".

Soweit die offizielle Verlautbarung. Man kann es allerdings auch so ausdrücken: Die Bundeswehr stellt sich für die Kriegsführung der Zukunft auf. Und diese Zukunft hat mit all ihren Bedrohungen und Risiken bereits begonnen.

Abseits der Hochglanz-Truppe
Berührt, belästigt, genötigt: Der Bundeswehr-Bericht des Verteidigungsministeriums zeigt, welche Soldaten besonders durch Übergriffe auffallen. Von Christoph Hickmann mehr ...

In den ersten neun Wochen des Jahres gab es 284 000 Angriffe auf Bundeswehr-Rechner

Schon jetzt sind die IT-Systeme der Bundeswehr massiven Angriffen ausgesetzt. Laut Bundeswehr wurden ihre Rechner in den ersten neun Wochen des Jahres mehr als 284 000 Mal attackiert. Man habe es bei der Cyber-Bedrohung "mit einer sehr ernst zu nehmenden Waffe zu tun", sagt Verteidigungs-Staatssekretärin Katrin Suder. Das liege auch daran, dass Cyber-Waffen "kostengünstig" seien und sich Angreifer schwer

zuordnen ließen. Daher, sagt Suder, sei das Cyber-Thema für sie "das Sicherheitsthema" schlechthin.

Die Bundeswehr stellt sich dieser Herausforderung nun mit ihrer neuen Cyber-Truppe, die künftig gleichberechtigt mit Heer, Luftwaffe und Marine agieren soll. Wobei man es sich nicht so vorstellen darf, dass auf einen Schlag Hunderte oder gar Tausende neue IT-Soldaten eingestellt würden. Stattdessen ist die Neuaufstellung vor allem eine Umstrukturierung und Bündelung vorhandener Kapazitäten - die allerdings für die Zukunft ausgebaut werden sollen.

So werden dem neuen Kommando zunächst lediglich 260 Soldaten angehören. Zum 1. Juli werden ihm dann mehrere Dienststellen und damit 13 500 Soldaten unterstellt. Bis 2021 sollen es nach Angaben des Kommandos fast 15 000 sein.

Knacken, sabotieren, ausschalten

Dabei handelt es sich keineswegs um 15 000 Hacker in Uniform. Stattdessen wird ein Großteil der Soldaten etwa für Schutz und Betrieb des IT-Systems der Bundeswehr zuständig sein. Doch es gibt eben auch eine kleine Einheit namens Computer-Netzwerk-Operationen, kurz CNO, die von 60 auf 80 Personen wachsen und tatsächlich "wirken" soll, wie das in der Militärsprache heißt - also im Zweifel Netzwerke knacken, sabotieren, ausschalten.

Das Thema ist heikel und hat bereits heftige Debatten ausgelöst, weshalb der neue Cyber-Inspekteur Ludwig Leinhos noch einmal besonders betont, dass es bei der Entwicklung offensiver Fähigkeiten nicht nur darum gehe, auch tatsächlich anzugreifen.

Stattdessen gebe es im Cyberraum eigentlich keinen Unterschied zwischen Offensive und Defensive: "Wenn Sie Ihre Systeme verteidigen wollen, müssen Sie auch wissen, wie ein potenzieller Angreifer agiert." Das Wissen darum, wie Angriffe funktionieren, könne in Krisensituationen "auch zur Analyse von Angriffen und zur Wiederherstellung der Funktionsfähigkeit der IT-Systeme genutzt werden".

Doch wann dürfte die Bundeswehr überhaupt tätig werden? Schließlich entscheidet hierzulande das Parlament über ihren Einsatz. Daran solle sich auch angesichts der Bedrohungen im Cyber-Raum nichts ändern, versichert das Verteidigungsministerium. "Wir agieren ausschließlich im Rahmen unserer Einsätze und des Mandats", sagt Staatssekretärin Suder. "Das ist kein rechtsfreier Raum."

Im Rahmen eines mandatierten Einsatzes aber kann eine Cyber-Operation durchaus eine attraktive Option sein. "Wenn wir auf diese Weise einen Gefechtsstand ausschalten können, vermeiden wir menschliche Opfer", sagt Generalleutnant Leinhos. "Wir bekommen eine Option, die Menschenleben schont."

Trotzdem gibt es Befürchtungen. Der Informatiker Thomas Reinhold vom Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg warnt, allein die Befähigung der Bundeswehr zu Offensivoperationen trage "ganz sicher nicht zu einer dringend gebotenen internationalen Abrüstung im Cyberspace bei".

Ähnlich klingt die Grünen-Abgeordnete Agnieszka Brugger: "Mit der Entscheidung für offensive Fähigkeiten gefährdet Ursula von der Leyen die Entwicklung eines freien und sicheren Internets und treibt die weltweite Aufrüstung im Netz voran." Von der Leyens "Kurswechsel" berge "erhebliche Gefahren und ein großes Eskalationspotenzial".

Für eine "Cyber-Reserve" sollen auch Experten aus der Industrie rekrutiert werden können

Es sind Grenzfragen, die sich aus der Cyber-Herausforderung ergeben - etwa danach, ob man überhaupt noch von einem Friedenszustand sprechen kann. Der Cyber-General Leinhos sagt es so: "Von dem Moment an, in dem Sie vernetzt sind, sind Sie ständig Ziel von Angriffen. Es wird keine Phase geben, wo IT-Infrastruktur nicht irgendwie attackiert wird." Es wäre "blauäugig", etwas anderes anzunehmen.

Die Frage sei, welche Qualität die Angriffe haben. Um Artikel 5 des Nato-Vertrags auszulösen, also den Bündnisfall, müsse "eine Schwelle überschritten werden, die bewusst nicht abschließend definiert ist". Ob die Voraussetzungen erfüllt seien, könne "nur im Einzelfall entschieden werden".

Kompetenzgerangel zwischen den Ministerien

Eine weitere Grenzfrage ist die nach der Zuständigkeit innerhalb der Bundesregierung. Die Grenzen zwischen innerer und äußerer Sicherheit verschwimmen angesichts der Cyber-Bedrohung - entsprechend intensiv war zwischenzeitlich das Kompetenzgerangel etwa zwischen Verteidigungs- und Innenministerium. Es sei "kein Geheimnis", dass es auch innerhalb der Bundesregierung Ressortdenken gebe, sagt Staatssekretärin Suder. "Aber das muss komplett überwunden werden."

Bleibt die Frage, ob der hehre Vorsatz durchzuhalten ist, wenn es darum geht, Nachwuchs zu gewinnen. Zwar entsteht gerade an der Bundeswehr-Universität München ein Studiengang "Cybersicherheit" samt Forschungszentrum. Zwar soll es eine "Cyber-Reserve" geben, um auf Experten auch aus der Industrie zurückgreifen zu können.

Trotzdem dürfte es sich kaum vermeiden lassen, dass etwa die Geheimdienste und die Bundeswehr künftig verschärft um geeignete Bewerber konkurrieren - die in der Industrie nach jetzigem Stand ein Vielfaches verdienen könnten. Derzeit wirbt die Bundeswehr mit Plakaten und Anzeigen großflächig um Cyber-Nachwuchs. "Wann darf man Hacker hacken?", so lautet die Frage auf einem der Plakate. Klingt fast, als sei sich die Truppe da selbst noch nicht ganz sicher.

Kaum ein Hacker will zum BND
Deutsche Geheimdienstler suchen verzweifelt IT-Spezialisten. Das Problem: Sie finden kaum jemanden. Die Kluft zwischen Hackern und Behörden erscheint unüberwindbar. Von Georg Mascolo, Reiko Pinkert, Ronen Steinke, Hakan Tanriverdi mehr...