Bundesministerium
der Verteidigung

-1880018-V53-

Bundesministerium der Verteidigung, 11055 Berlin

Vorsitzenden
des Verteidigungsausschusses
des Deutschen Bundestages
Herrn Wolfgang Hellmich, MdB
Platz der Republik 1
11011 Berlin

Markus Grübel
Parlamentarischer Staatssekretär
Mitglied des Deutschen Bundestages

HAUSANSCHRIFT Stauffenbergstraße 18, 10785 Berlin
POSTANSCHRIFT 11055 Berlin

TEL +49 (0)30 2004-22400
FAX +49 (0)30 2004-22441
E-MAIL BMVgBueroParlStsGruebel@BMVg.Bund.de

Deutscher Bundestag
Verteidigungsausschuss

Ausschussdrucksache
18(12)603

07.01.2016 - 18/2562

5420-4

Berlin, 6. Januar 2016

Sehr geehrter Herr Vorsitzender,

in der 48. Sitzung des Verteidigungsausschusses des Deutschen Bundestages am 14. Oktober 2015 haben die Fraktionen das Bundesministerium der Verteidigung gebeten, eine Bestandaufnahme möglicher Angriffsmöglichkeiten, Gefährdungen und Kompromittierungen der Informations- und Kommunikationsinfrastruktur der Bundeswehr und mögliche Abwehrkonzepte in geeigneter Art und Weise vorzulegen. Des Weiteren wurde gebeten, darzulegen,

- wie viele IT-Spezialisten das sogenannte „Kommando für den Cyberinforaum" insgesamt umfassen soll und wie viele IT-Spezialisten der Bundeswehr fehlen, um das neue Kommando aufzubauen,
- welche finanziellen Mittel für einen entsprechenden Personalaufwuchs im Haushalt bereit zu stellen seien und wie besondere Anreize für die Gewinnung von hochqualifizierten IT-Spezialisten ausgestaltet sein könnten und
- welche Kosten für die technische Ausstattung des „Kommandos für den Cyberraum" zu erwarten sind.

Die Bundeswehr richtet seit 2013 den Schutz ihrer IT-Systeme an den Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI) aus. Dieser Standard wird „IT-Grundschutz" genannt.

Das BSI hat in seiner für Cybersicherheit in der Bundesverwaltung federführenden Rolle mit dem „IT-Grundschutz“ ein international anerkanntes und genutztes Kompendium für den gesamten IT-Sicherheitsmanagementprozess geschaffen. Der IT-Grundschutz beschreibt im Einzelnen und in allgemein gültiger Form mögliche Gefährdungen und diesen zugeordnete Abwehrmaßnahmen. Daher wendet die Bundeswehr den IT-Grundschutz auch für das IT-System der Bundeswehr an.
Bei hohem und sehr hohem Schutzbedarf für die Vertraulichkeit (Geheimschutz) und für die Verfügbarkeit und Integrität von Informationen bzw. von IT werden in der Bundeswehr Bedrohungen und Abwehrmaßnahmen berücksichtigt, die über den IT-Grundschutz hinausgehen. Diese sind in der zentralen Dienstvorschrift „IT-Sicherheit in der Bundeswehr“ beschrieben. Auch in diesem Fall richten sich die Gefährdungsanalyse und der gesamte IT-Sicherheitsmanagementprozess an der IT-Grundschutzmethodik aus. Der IT-Grundschutz des BSI befindet sich im Übrigen derzeit in der Endphase eines umfangreichen Reformprozesses. Das Verteidigungsressort, konkret das Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw), begleitet diesen Reformprozess eng.

Eine besondere Bedrohung stellen in zunehmender Weise zielgerichtete Angriffe und insbesondere hoch spezialisierte Angriffe, sogenannte „Advanced Persistant Threats“ (APT), dar. Diese zielen unter anderem darauf ab, dass der Angegriffene den Angriff und den erzeugten Schaden möglichst lange nicht erkennt. Es muss davon ausgegangen werden, dass nachrichtendienstliche Erkenntnisse in die Entwicklung eines APT einfließen. Es kann nicht ausgeschlossen werden, dass Hersteller von IT-Produkten an der Entwicklung von APTs mitwirken oder diese zumindest dulden. Dies bedeutet jedoch auch, dass die Entwicklung oder Beschaffung eines APT mit hohen (Erkennungs-)Risiken verbunden ist. Ein vollständiger Schutz gegen APTs ist grundsätzlich nicht möglich.
Für das IT-System der Bundeswehr bestehen Abwehrkonzepte, die weitestgehend aus den Vorgaben des IT-Grundschutzes abgeleitet sind. Abwehrkonzepte gegen Bedrohungen im Cyberraum müssen über den gesamten Lebenszyklus eines IT-Systems bzw. eines IT-Services wirken und sind daher unmittelbar bei deren Entwicklung zu berücksichtigen. Ein wichtiges Abwehrkonzept ist das sogenannte „Patchmanagement“, da nur sehr wenige schwachstellenfreie IT-Systeme existieren und im Lebenszyklus eines IT-Systems erkannte Schwachstellen zeitnah und in geeigneter Weise beseitigt bzw. abgesichert werden müssen.

Allerdings eröffnet das Patchmanagement Möglichkeiten für potenzielle Manipulationen und Angriffe bis hin zu APTs. Darüber hinaus sind Abwehrkonzepte stets mehrstufig aufgebaut (Prinzip der „Verteidigung in der Tiefe"), so dass bei erfolgreichem Umgehen eines technischen „Hindernisses" weitere Maßnahmen wirksam und eine angemessene Sicherheit des Systems oder Services bzw. der dort verarbeiteten Informationen gewährleistet werden kann. Hierzu gehören insbesondere auch Maßnahmen einer möglichst umfassenden und lückenlosen Überwachung eines IT-Systems nach innen (anhand des definierten Normverhaltens eines Systems) sowie an den Schnittstellen nach außen (durch technische Schutzmaßnahmen wie Firewalls, Gateways, Proxiserver, Intrusion Prevention, etc.). Die Abwehrkonzepte und die daraus resultierenden Maßnahmen müssen kontinuierlich mit der schnell fortschreitenden Entwicklung der Informationstechnologie auf ihre Wirksamkeit hin überprüft und angepasst werden.
Neue Abwehrkonzepte, die über den rein passiven, technischen Schutz und die reaktiven Maßnahmen zur Minimierung der Auswirkungen eines Angriffes sowie die Wiederherstellung von IT-Systemen hinausgehen, wurden durch das NATO Cooperative Cyber Defence Center of Excellence (CCD CoE) in Tallinn/Estland im Rahmen der Studie „Responsive Cyber Defence – technical and legal analysis", „Insider Threat Detection" und „Anti Forensic Measures" untersucht. Die Ergebnisse zu „Responsive Cyber Defence" werden derzeit in der NATO diskutiert und weiter untersucht. Ziel ist es, Möglichkeiten zur Unterbindung oder Beendigung eines Angriffes unter Berücksichtigung der rechtlichen Rahmenbedingungen zu identifizieren und, wenn im Einzelfall möglich, anzuwenden. Sobald für solche Abwehrkonzepte für den Einsatz in der Bundeswehr ein justiziabler Rahmen gefunden werden kann, ist vorgesehen, diese in der Bundeswehr auszuplanen und umzusetzen. Der Bedarf an fortgeschrittenen Abwehrkonzepten für die Bundeswehr, unter anderem unter Berücksichtigung von Security Analytics, Advanced Defence sowie der Nutzung und Verarbeitung von Big-DATA wurde identifiziert und wird in der derzeit in Erarbeitung befindlichen Umsetzung der „Strategischen Leitlinie Cyber-Verteidigung im Geschäftsbereich BMVg" ausgeplant. Zum Teil sind solche Methoden bereits heute Bestandteil der in der Bundeswehr verwendeten Sicherheitsprodukte (Firewalls, Virenschutz, etc.) und damit Bestandteil des Gesamtabwehrkonzepts.

Um besondere Anreize für die Gewinnung von hochqualifiziertem IT-Personal auszugestalten, werden derzeit verschiedene Möglichkeiten für neue Wege der Personalgewinnung, -entwicklung und -bindung geprüft. Dabei sollen unter anderem sowohl monetäre als auch nicht-monetäre Ansatzpunkte aus dem Gesetz zur Steigerung der Attraktivität des Dienstes in der Bundeswehr (BwAttraktStG) in die Überlegungen einbezogen werden. Eine endgültige Entscheidung über die Realisierung dieser Personalgewinnungsmaßnahmen steht derzeit allerdings noch aus.

Die durch Frau Bundesministerin angekündigten, organisatorischen Veränderungen im Geschäftsbereich des Bundesministeriums der Verteidigung werden derzeit durch einen Aufbaustab „Cyber- und Informationsraum" erarbeitet, der im November 2015 in der Verantwortung von Frau Staatssekretärin Dr. Suder eingerichtet wurde. Der Aufbaustab soll seine Arbeit bis Frühjahr 2016 abschließen und Frau Bundesministerin einen Bericht zum Aufbau eines eigenständigen Organisationselementes „Cyber/IT" im Ministerium und eines neuen Organisationsbereiches unter einem Kommando „Cyber- und Informationsraum" in unmittelbarer Unterstellung zum Ministerium vorlegen. Einzelheiten zu Strukturen und folglich auch zu Personalumfängen werden Gegenstand der Untersuchungen sein. Dasselbe gilt für Angaben zu Finanzmitteln, die ggf. für einen Personalaufwuchs oder die technische Ausstattung des Kommandos „Cyber- und Informationsraum" benötigt werden.

Mit freundlichen Grüßen

Markus Grübel