

## **Bundesministerium der Verteidigung (BMVg)**

(Einzelplan 14)

### **24 Bundeswehr gefährdet die IT-Sicherheit in technischen und wissenschaftlichen Dienststellen**

(Kapitel 1413)

#### **Zusammenfassung**

*In technischen und wissenschaftlichen Dienststellen der Bundeswehr bestehen seit Jahren Sicherheitsmängel bei der IT. Der Bundesrechnungshof sieht dadurch die zuverlässige Aufgabenerfüllung der Dienststellen gefährdet. Zu ihren wesentlichen Aufgaben gehört es, das für die Bundeswehr vorgesehene Material zu untersuchen und zu bewerten. Das zuständige Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr hat die Mängel eingeräumt. Allerdings hat es bisher keine ausreichenden Anstrengungen unternommen, um die Risiken zu verringern. Dafür fehle ihm geeignetes Personal. Der Bundesrechnungshof erwartet vom BMVg, dass es die IT-Sicherheitsmängel schnellstmöglich beseitigt. Dafür sollte es den Dienststellen für die besonders wichtigen IT-Sicherheitsaufgaben ausreichend Personal bereitstellen. Es muss darüber hinaus dafür sorgen, dass dieses Personal hinreichend ausgebildet ist und über geeignete Unterstützungssoftware verfügt.*

#### **24.1 Prüfungsfeststellungen**

Der Bundesrechnungshof prüfte die IT in Dienststellen des Bundesamtes für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (Bundesamt). Diese technischen und wissenschaftlichen Dienststellen unterstützen mit ihrer Fachexpertise das Bundesamt dabei, die Bundeswehr mit geeignetem Material auszurüsten. Die Dienststellen sind jeweils für bestimmte Ausrüstungsbereiche zuständig. Sie verfügen über spezielle Kenntnisse und Fähigkeiten, z. B. in der Fahrzeug-, Luftfahrt- und Schiffstechnik sowie in den Bereichen Elektronik, Munition, Werkstoffe und Schutztechnologien. Um ihre Aufgaben erfüllen zu können, sind die Dienststellen auf eine sicher funktio-

nierende IT angewiesen. Sie müssen IT-Sicherheitsvorschriften der Bundeswehr einhalten, die auf den Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik aufbauen.

### **Wesentliche Mängel**

Neben Mängeln bei der Beschaffung, dem Betrieb und der Verwaltung von IT stellte der Bundesrechnungshof bei seiner Prüfung gravierende konzeptuelle, betriebliche und technische Mängel der IT-Sicherheit in den Dienststellen fest. So hatten die Dienststellen weder untersucht noch festgelegt, welcher Schutz für ihre Geschäftsprozesse, die dabei verarbeiteten Informationen und die eingesetzte IT überhaupt angemessen ist. Die Dienststellen verfügten über keine anwendbaren Konzepte oder ausreichend detaillierte Vorgaben zu notwendigen IT-Sicherheitsmaßnahmen.

Dienststellen ließen Teile ihrer IT nicht durch hierfür ausgebildetes IT-Fachpersonal, sondern von den Nutzerinnen und Nutzern selbst administrieren. Damit setzten sie sich dem Risiko aus, ihre IT aufgrund fehlerhafter Konfiguration, unkontrolliert installierter Software oder unzureichender Sicherheitsupdates mit Schadsoftware zu infizieren.

Die Dienststellen protokollierten sicherheits- und datenschutzrelevante Ereignisse in ihren IT-Systemen nicht in erforderlichem Umfang. Die aufgezeichneten Protokolldaten werteten die Dienststellen nur ansatzweise aus („Auditing“). So konnten die Dienststellen sicherheitskritische Ereignisse oder Datenschutzverstöße beim Betrieb ihrer IT weder erkennen noch Gegenmaßnahmen ergreifen.

Diese und weitere IT-Sicherheitsmängel bestanden zu großen Teilen bereits mehrere Jahre. Auch die zuständige bundeswehrinterne Kontrollinstanz hatte in den letzten Jahren mehrfach berichtet, dass in technischen und wissenschaftlichen Dienststellen die IT-Sicherheit nicht gewährleistet war.

### **Personal**

In den für IT zuständigen Organisationseinheiten waren Dienstposten teilweise seit Jahren unbesetzt. Dadurch war das Personal oft überlastet. Es

orientierte sich zwar an den IT-Sicherheitsvorschriften der Bundeswehr, war aber vielfach nicht in der Lage, die wesentlichen Bestimmungen einzuhalten. Dazu fehlte dem IT-Personal oft eine ausreichende Ausbildung und geeignete Unterstützungssoftware. Dies galt auch für das Personal, das in den Dienststellen mit der Gewährleistung und mit der Prüfung der IT-Sicherheit beauftragt war.

## **24.2 Würdigung**

Der Bundesrechnungshof hat beanstandet, dass die Dienststellen gegen Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik und IT-Sicherheitsvorschriften der Bundeswehr verstoßen haben. Die daraus resultierenden IT-Sicherheitsmängel haben dazu geführt, dass der IT-Betrieb der Dienststellen erheblichen Gefahren ausgesetzt ist. Dadurch hat sich nach Ansicht des Bundesrechnungshofes auch eine Gefahr für den Dienstbetrieb insgesamt und damit für die zuverlässige Aufgabenerfüllung der Dienststellen ergeben.

Der Bundesrechnungshof hat deshalb das Bundesamt aufgefordert, die festgestellten Mängel zu beheben. Dabei hat er u. a. empfohlen, ausreichendes Personal bereitzustellen sowie das IT-Sicherheitspersonal so auszubilden und mit geeigneter Unterstützungssoftware auszustatten, dass es seine Aufgaben angemessen wahrnehmen kann.

## **24.3 Stellungnahme**

Das Bundesamt hat eingeräumt, dass die Feststellungen des Bundesrechnungshofes im Wesentlichen zutreffen. Es habe erste Schritte unternommen, die Empfehlungen umzusetzen. So habe es z. B. geplant, Dokumentationsvorlagen und Mindestvorgaben für den Betrieb besonders gefährdeter IT zusammenzustellen und anzuweisen. Es hat dabei ausgeführt, dass eine Umsetzung davon abhängig sei, ob ausreichend Personal zur Verfügung gestellt werden könne.

Das Bundesamt habe auch geplant, eine Initiative zur Erstellung eines bundeswehrweiten „Auditingrahmenkonzeptes“ zu starten, auf das die Dienststellen aufbauen könnten. Es hat dazu weiter ausgeführt, dass für eine Umsetzung die aktuelle Personallage in den Dienststellen keinen Raum lasse.

Das Bundesamt ist in seiner Stellungnahme nicht darauf eingegangen, wie es dafür sorgen will, dass seinen Dienststellen künftig ausreichendes IT-Personal zur Behebung der IT-Sicherheitsmängel zur Verfügung steht.

Das BMVg hat die ausreichende Ausstattung der Dienststellen mit hinreichend ausgebildetem IT-Personal als Schlüssel zur Umsetzung der Empfehlungen des Bundesrechnungshofes erkannt. Hierzu hat es darauf hingewiesen, dass es mit der „Trendwende Personal“ erreicht habe, dass der Dienstpostenumfang der betroffenen Dienststellen derzeit aufwachse. Es hat weiter ausgeführt, dass die Bundeswehr mit ihrer „Attraktivitätsagenda“ neue Wege einschlage, um im Wettbewerb mit der Industrie Dienstposten für IT-Fachkräfte besetzen zu können.

Das BMVg hat auch dargelegt, dass das Bundesamt kurzfristig weitere Maßnahmen ergriffen habe, um IT-Sicherheitsrisiken zu begegnen. So habe es *„die Einrichtung von geschulten IT-Sicherheitsgehilfen in allen Abteilungen des Bundesamtes als first point of contact in Fragen der Informationssicherheit“* vorgesehen. Dies ermögliche *„eine Entlastung des Bereiches IT-Sicherheit des Bundesamtes und dadurch die Generierung von Kapazitäten für die Unterstützung der IT-Sicherheit der Dienststellen.“* Das BMVg hat weiter dargelegt, dass regelmäßig alternative Wege zur Gewährleistung der IT-Sicherheit geprüft würden. So werde überlegt, eine bereits in der Bundeswehr vorhandene Unterstützungssoftware weiterentwickeln zu lassen. Diese würde das IT-Sicherheitspersonal der Dienststellen bei der Bearbeitung von IT-Sicherheitskonzepten unterstützen und sie somit entlasten.

#### **24.4 Abschließende Würdigung**

Der Bundesrechnungshof erkennt an, dass das Bundesamt erste Schritte in die richtige Richtung gemacht hat. Er hält die bisherigen Anstrengungen des

Bundesamtes zur Behebung der IT-Sicherheitsmängel in seinen Dienststellen jedoch noch immer für unzureichend.

Auch die Bemühungen des BMVg, ausreichend Personal für einen sicheren IT-Betrieb bereitzustellen, es angemessen auszubilden und mit geeigneter Unterstützungssoftware auszustatten, sind allenfalls ein erster Schritt. Besonders schwer wiegt, dass die kritische Situation der IT-Sicherheit und auch die kritische Situation beim IT-(Sicherheits-)Personal durch bundeswehrinterne Berichte seit Jahren bekannt sind.

Das BMVg richtet zwar mit der „Trendwende Personal“ zusätzliche Dienstposten bei den Dienststellen ein. Diese Maßnahme bleibt aber wirkungslos, so lange nicht einmal bereits vorhandene Dienstposten mit qualifiziertem Personal besetzt werden können. Der Bundesrechnungshof kann bisher ebenfalls nicht erkennen, dass die „Attraktivitätsagenda“ zu einer signifikanten Verbesserung der Situation beim IT-Sicherheitspersonal der Dienststellen des Bundesamtes führt.

Auch die vom Bundesamt vorgesehenen Maßnahmen können dem grundsätzlichen Personalproblem bestenfalls in geringem Umfang entgegenwirken. Die sogenannten IT-Sicherheitsgehilfen im Bundesamt mögen zwar sinnvoll sein. Die Auswirkungen auf die Situation in den Dienststellen des Bundesamtes bleiben allerdings abzuwarten.

Insofern zeigt die Bundeswehr aus Sicht des Bundesrechnungshofes noch immer keine erfolgversprechenden Wege auf, die Mängel bei der IT-Sicherheit und insbesondere beim IT-Sicherheitspersonal konsequent abzustellen. Hierdurch gefährdet sie weiter und in zunehmendem Maß den ordnungsgemäßen IT-Betrieb und damit die Voraussetzung für die zuverlässige Aufgabenerfüllung der Dienststellen des Bundesamtes.

Der Bundesrechnungshof erwartet, dass das BMVg das Bundesamt stärker dabei unterstützt, die Empfehlungen des Bundesrechnungshofes zeitnah umzusetzen. Er erwartet vor allem konkretere Schritte beim Personalmanagement, damit den Dienststellen zügig Personal bereitsteht, um einen

sicheren IT-Betrieb gewährleisten zu können. Dabei sollte die Bundeswehr den aktuellen Bedarf an IT-Betriebspersonal und IT-Sicherheitspersonal nach anerkannten Methoden ermitteln. Die Bundeswehr muss darüber hinaus dafür sorgen, dass dieses für den sicheren IT-Betrieb erforderliche Personal hinreichend ausgebildet ist und über geeignete Unterstützungssoftware verfügt.

Sollte die Bundeswehr das erforderliche zusätzliche Fachpersonal dauerhaft nicht gewinnen können, muss das BMVg weitere Wege zur Gewährleistung der IT-Sicherheit entwickeln (z. B. Qualifikation oder Umschulung eigenen Personals für IT-Aufgaben, Automatisierung von Tätigkeiten, Einsatz Externer usw.). Sollte dies nicht möglich sein, muss die Bundeswehr für den Einsatz ihres vorhandenen IT-Personals die Prioritäten verändern.