Informationssicherheit in der Armee

Autor(en): **Winzer, Ralf**

Objekttyp: **Article**

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

Band (Jahr): **181 (2015)**

Heft 9

PDF erstellt am: **17.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-583219

Informationssicherheit in der Armee

Die abstrakte, immaterielle Natur von Informationen und deren Übertragung sowie die als selbstverständlich wahrgenommene allgegenwärtige Verfügbarkeit von ICT-Diensten erschweren das Verständnis für die Abhängigkeit der Gesellschaft – darunter subsumieren wir auch die Landesverteidigung – von einer funktionierenden und integren Informationsinfrastruktur massgeblich.

Ralf Winzer

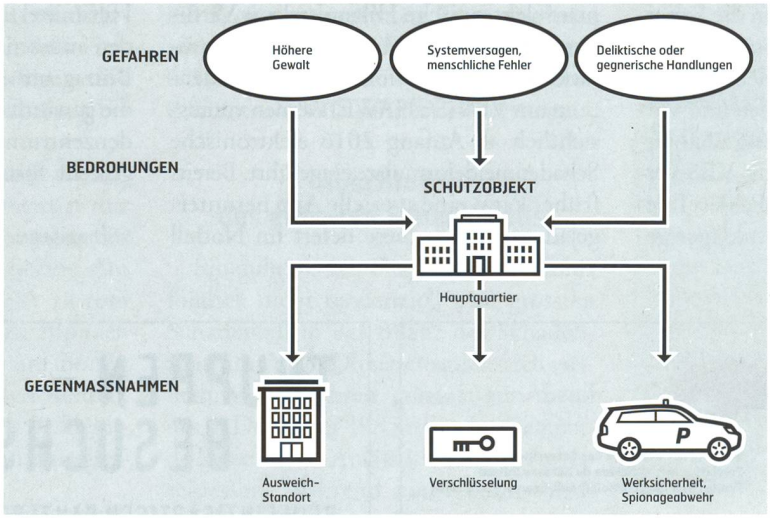
Der Stellenwert von Informationen und des Einsatzes von Kommunikationstechnologien hat in der Landesverteidigung ebenso wie in der Wirtschaft, bei Behörden, aber auch für die Grundversorgung und im Privatleben in den letzten Jahren enorm zugenommen. Die Möglichkeit, schnell und überall Informationen übermitteln oder erhalten zu können, lässt uns immer mehr vergessen, wie abhängig wir sowohl im militärischen wie zivilen Umfeld tatsächlich von diesem immateriellen, nicht physisch fassbaren Gut namens Information geworden sind. Entsprechend schwer fassbar sind die Bedrohungen und deren Folgen, die auf die ICT-Infrastruktur einwirken können. Die sich daraus ergebenden Risiken müssen erst mittels geeigneter Verfahren und Methoden fassbar und messbar gemacht werden.

Wovor müssen Informationen und deren Übertragung geschützt werden?

Bezüglich sensibler Informationen kommen einem dazu unmittelbar Begriffe wie Datenschutz, Verschlüsselung und Schutz vor unerwünschtem Abhören und Mithören in den Sinn. Jeder Angehörige der Armee (AdA) und das Kader im Besonderen wurden in ihrer Ausbildung über den Umgang mit klassifizierten Informationen und die Anforderungen an die Geheimhaltung instruiert.[1] Doch sind dies die einzigen schützenswerten Aspekte? In der Informationssicherheit werden üblicherweise vier *Schutzziele* betrachtet:

Vertraulichkeit:

Massnahmen, damit Informationen und Kommunikationsinhalte nicht in den Besitz von unerwünschten Stellen gelangen: Zu den gängigen Massnahmen zählen dabei die Verschlüsselung von Übertragungskanälen und Datenspeichern, aber auch das Einschliessen von sensiblen Dokumenten oder Zurückhaltung beim Besprechen heikler Themen in der Öffentlichkeit. Die Vertraulichkeit wird üblicherweise gemäss vordefinierten Stufen eingeteilt. Die 2007 in Kraft getretene Informationsschutzverordnung (ISchV) vereinheitlicht und vereinfacht die Klassifizierung innerhalb der Bundesverwaltung und der Schweizer Armee: Das Schutzziel der Vertraulichkeit unterscheidet zwischen den Klassifikationsstufen GEHEIM, VERTRAULICH und INTERN (Art. 4 ISchV). Die in anderen Kulturkreisen als SECRET und TOP SECRET eingestuften Informationen und Anlagen werden in der Schweiz bei Bund und Armee als GEHEIM bezeichnet; ihre Kenntnisnahme durch Unberechtigte kann den Landesinteressen einen schweren Schaden zufügen. Als VERTRAULICH gelten Informationen, deren Kenntnisnahme durch Unberechtigte den Landesinteressen sonstigen Schaden zufügen kann. Die im englischsprachigen Raum anzutreffende Einstufung RESTRICTED fällt in der Schweiz unter INTERN. Es handelt sich hierbei um Informationen mit erhöhtem Schutzbedarf, die weder als GEHEIM noch als VERTRAULICH klassifiziert werden müssen. Sämtliche Informationen und Anlagen, die nicht explizit einer dieser drei Stufen zugeordnet sind, gelten als UNKLASSIFIZIERT.



Gefahren, Bedrohungen und Gegenmassnahmen. Grafik: Crypto AG

Integrität:

Massnahmen, damit Informationen vollständig und unverändert übermittelt bzw. empfangen werden können: Inhalte sollen hierdurch weder durch Systemfehler oder Übertragungsprobleme noch durch mutwillige Veränderung beeinträchtigt werden können. Wenn nicht nur die Information selber, sondern auch die relevanten Randdaten wie Absender oder Autor, Empfängernamen, Versand- und Empfangszeitpunkt usw. gegen Manipulation geschützt werden, werden die entsprechenden Massnahmen als *Authentizität* bezeichnet. Gängige Mechanismen hierzu sind elektronische Signaturen.

Verfügbarkeit:

Massnahmen, damit Informationen und Kommunikationskanäle im Bedarfsfall verfügbar sind: Informationen sind hierbei sowohl vor Verlust und Zerstörung als auch vor Unzugänglichkeit zu schützen. Bewährte Vorkehrungen sind Backup-Systeme, die Archivierung von wichtigen Dokumenten an einem sicheren Ort oder die redundante Auslegung von Übertragungswegen.

Nachvollziehbarkeit:

Massnahmen, damit die Einhaltung der geltenden regulatorischen Auflagen nicht nur sichergestellt, sondern auch revisionstauglich überprüft und nachgewiesen werden kann: Typischerweise werden zur Wahrung der Nachvollziehbarkeit Audit-Trails angefertigt, Kontrollmassnahmen durchgeführt und periodische Audits durch unabhängige Stellen vorgenommen. Im Militärbereich unterliegt unter Umständen der Einsatz gewisser Waffensysteme und die Durchführung gewisser Kampfhandlungen (Langstrecken-Marschflugkörper, Fliegereinsätze, Spezialmissionen) bestimmten Protokollierungspflichten.

Die Bewertung und Einstufung des Schutzbedarfs gemäss den oben aufgeführten Schutzzielen für einen Informationsbestand oder ein ICT-System wird als *Klassifizierung* bezeichnet. Die Informationsschutzverordnung behandelt leider von den vier obigen Schutzzielen ausschliesslich die Vertraulichkeit. Zudem führt der Grundsatz, dass alle Informationen ohne expliziten Klassifizierungsvermerk als UNKLASSIFIZIERT (und somit implizit als nicht schutzbedürftig) gelten, dazu, dass viele Daten unzureichend geschützt werden. In der Privatwirtschaft kann davon ausgegangen werden, dass die überwiegende Mehrheit aller Informationen als INTERN betrachtet werden. Bei Behörden und Armee sind ungefähr 6% der Informationen als INTERN, 3% als VERTRAULICH und 1% als GEHEIM klassifiziert.

Risiken in Zusammenhang mit der Informationssicherheit

Die Ermittlung der Bemessung von Risiken der Informationssicherheit erfolgt gemäss der sogenannten Risikomatrix, wie sie bereits in anderem Zusammenhang vortrefflich in der ASMZ Nr. 05/2015 beschrieben worden ist.[2]

Die Risiken in der Informationssicherheit ergeben sich hauptsächlich aus den drei Gefahrenbereichen höhere Gewalt, Systemversagen bzw. menschliche Fehler sowie deliktische (inkl. gegnerische) Handlungen.

Leistungsfähige Verschlüsselungssysteme, wie sie die Crypto AG anbietet, sind und bleiben unverzichtbare Massnahmen zur Wahrung der Informationssicherheit innerhalb der Landesverteidigung.

Mehr noch obliegt es jedem einzelnen AdA, insbesondere den höheren Chargen, durch ihr aufmerksames Verhalten sowohl im Umgang mit den elektronischen Mitteln im Dienstbetrieb und bei vordienstlichen Tätigkeiten als auch bei der mündlichen Kommunikation – zum Beispiel am Handy – der Informationssicherheit Sorge zu tragen. Die Sicherheit von Informationen bildet ebenso wie der Schutz der physischen militärischen Einrichtungen einen tragenden Pfeiler zur Wirksamkeit der Landesverteidigung. ■

1 Siehe auch Merkblatt für Geheimnisträger 2.4a des VBS.

2 Br D. Keller, Oberstlt i Gst C. Oberlin, «Erst wägen, dann wagen: Umgang mit Risiken in der Führung».

Ralf Winzer
Ing. informaticien EPFL
Customer Segment Manager
Crypto AG
6301 Zug