IAM-Degradation im militärischen Umfeld

Studiengang: EMBA Innovation Management

Die IKT-Systeme des VBS liefern in mannigfaltiger Hinsicht die IAM-Basis zur Einsatz- und Durchhaltefähigkeit der Schweizer Armee im Einsatz. Hierzu muss der autarke IKT-Betrieb im Einsatz und die Audit- bzw. Revisionsfähigkeit nach dem Einsatz mittels IAM-Degradation gewährleistet sein. Die Master Thesis soll hierfür mögliche Lösungsansätze aufzeigen.

Ausgangslage

Im Bereich IKT des Verteidigungsdepartements VBS werden unterschiedlichste Silos von Verzeichnisdiensten zur Verwaltung von digitalen Identitäten sowie zur Regelung von Benutzerzugriffen und Benutzerrechten auf Systeme und Anwendungen genutzt. Diese Verzeichnisdienste müssen parallel betrieben werden, was zu einem hohen Aufwand führt.

Mittels eines zentrales Identity Access Management Systems kommt ein übergreifendes Verwaltungsinstrument zum Einsatz, welches die verschiedenen Verzeichnisdienste managen und Identitäten mit Partner-Organisationen föderieren kann. Das physische Zutrittsmanagement wird ebenfalls mit Identitäten beliefert und ermöglicht so das zentrale Management der Ausweise und der Gebäudezutritte.

Das Zusammenspiel aller Systeme muss in allen Klassifizierungsebenen und Schutzklassen zur Verfügung stehen. Dazu ist es notwendig, dass die Lösung im autarken Führungsnetz der Armee betrieben wird. Im Gegensatz zur zivilen Welt muss ein militärisches Identity Access Management System in allen Lagen funktionieren. Hierbei wird zwischen normaler, besonderer und ausserordentlicher Lage unterschieden.

Ziel

Das Ziel der Arbeit war, aus den Ergebnissen und Erkenntnissen Aufschlüsse über die zur Erfüllung der Anforderungen notwendigen Massnahmen zu liefern und dem geforderten Verfügbarkeitsniveau Rechnung zu tragen.

Die Ergebnisse sollen nicht nur die technischen Aspekte berücksichtigen, sondern auch die Organisatorischen und Prozessualen.

Vorgehen

Nach der Analyse der systemischen, normativen und organisationellen Grundlagen wurde zuerst eine aktuelle Situationsbeurteilung durchgeführt. Mittels Befragungen der zivilen und militärischen Stakeholder und Experten konnten Stossrichtungen erforscht und Handlungsfelder definiert werden. Verifiziert wurden diese mittels vertieftem Studium und Recherchen eingängiger Fachliteratur, relevanter Publikationen und der vorhandenen Best-IT-Practices.

Aus den Resultaten konnten die Schwerpunkte herauskristallisiert und aufgrund vertiefter Untersuchungen der Risiken die Lösungsansätze konkretisiert werden. Diese konnten anschliessend spezifisch ausgearbeitet und auf die Umsetzbarkeit überprüft werden. Letztendlich wurden die zur Umsetzung notwendigen Schritte für die Implementierung in Handlungsempfehlungen festgehalten.

Erkenntnisse

Für die Degradation ist im militärischen Umfeld ein autarker Betrieb der IKT-Identitäts-Systeme sicherzustellen. Um eine regelkonforme, auditfähige und sichere Rückführung der IKT-Systeme mit den militärischen Identitäten der Armee zu gewährleisten, sind mehrere Faktoren einzubeziehen. Eine vollständige Implementation muss auf unterschiedlichsten Stufen entlang der rechtlichen und normativen Vorgaben der beteiligten Organisationen erfolgen. Daher ist sie keineswegs trivial, sondern eine grosse Herausforderung, muss sie doch unterschiedlichste komplexe Anforderungen erfüllen. Es bedarf festzulegender Rahmenbedingungen, welche in der Arbeit erforscht und beschrieben wurden.

Bernhard Pulfer