EDV-Projekt „OrgFlex“ gestoppt

Die Bundesheergewerkschaft warnt seit Jahren davor. Nun wurde die Einführung und Produktivsetzung von „OrgFlex“, einem Großrechnerprogramm im Bundesheer, gestoppt.

Vorauszuschicken ist: Für die Datensicherheit und die Prüfung externer Dienstleister in Fragen solcher EDV-Systeme ist das Heeresabwehramt verantwortlich. Der Leiter des Heeresabwehramtes ist der IKT-Sicherheitsbeauftragte des Verteidigungsministers. Und anscheinend liegen dort Sicherheitsbedenken vor. Brisant ist dies deshalb, weil es im Innenressort aktuell einen Sicherheitsvorfall mit einem externen Dienstleister gibt, wo scheinbar unberechtigte Zugriffe auf Daten erfolgten.

Im Verteidigungsressort laufen auf den Großrechnern verschiedene Systeme für die Personalverwaltung, Versorgung, Verwaltung und für die Einsatzvorbereitung des Bundesheeres. Mit OrgFlex sollten nun neue Systeme mit Echtdaten von mehr als 20.000 Soldaten und Bediensteten in den sogenannten Produktionsbetrieb gehen. Dies bedeutet, dass es nach einer Testphase einen realen Datentransfer in das Bundesrechenzentrum (BRZ) des Finanzministeriums gegeben hätte. Zunächst ist das auch noch nicht außergewöhnlich, zumal schon jetzt verschiedene Systeme bestehen, die mit gleichartigen Großrechnersystemen im Bundesheer in Zusammenarbeit mit dem BRZ bearbeitet werden, wie etwa die Dienstreiseabrechnung oder die Besoldung. OrgFlex setzt jedoch neue Maßstäbe, sowohl in Bezug auf die Komplexität, als auch in Bezug auf die Datenmengen. Und zudem ist es mit der neuen Zeitordnung (Überstunden, Zeitkarte, Dienstplan) verknüpft.

Foto: pixabay.com

Bundesheer ist ein besonderes Ressort mit besonderen Personaldaten

Das Verteidigungsressort kann nicht mit anderen Ministerien der Republik gleichgestellt oder verglichen werden. Es hat sensible Sonderdienststellen, wie das Heeresnachrichtenamt (Auslandsdienst), das Heeresabwehramt (Inlandsdienst), die Einsatzsoldaten des Jagdkommandos, die Militärpolizei und den sogenannten S2-Sicherheitsdienst. Aber auch unsere Soldaten und Bediensteten in den Kampfverbänden im In- und Ausland unterliegen einem besonderen Schutz – vom Aufklärungssoldaten bis hin zum Eurofighter-Piloten. Die Soldaten und Bediensteten im Verteidigungsressort haben im Vergleich zu anderen Ministerien ein sehr umfangreiches digitales Personaldatenblatt mit Gesundheitsdaten, Einsatzdaten, Sprach- und Ausbildungsprofilen, mit Waffenausbildungen und mit Einträgen zur Einsatzbereitschaft und zu Sonderausbildungen. Und diese sensiblen Daten gilt es zu schützen! Der Bundesheergewerkschaft sind die Daten der Bediensteten heilig! Und deshalb ist es ein langjähriges Anliegen, dass die Datenschutzrichtlinien und die Bestimmungen des Personalvertretungsgesetzes auf Strich und Punkt eingehalten werden. Die AUF/AFH hat so etwa auch eingebracht, dass mit der Einführung der neuen Zeitordnung beim „Dienstplan“ das jeweils zuständige PV-Organ einzubinden ist.

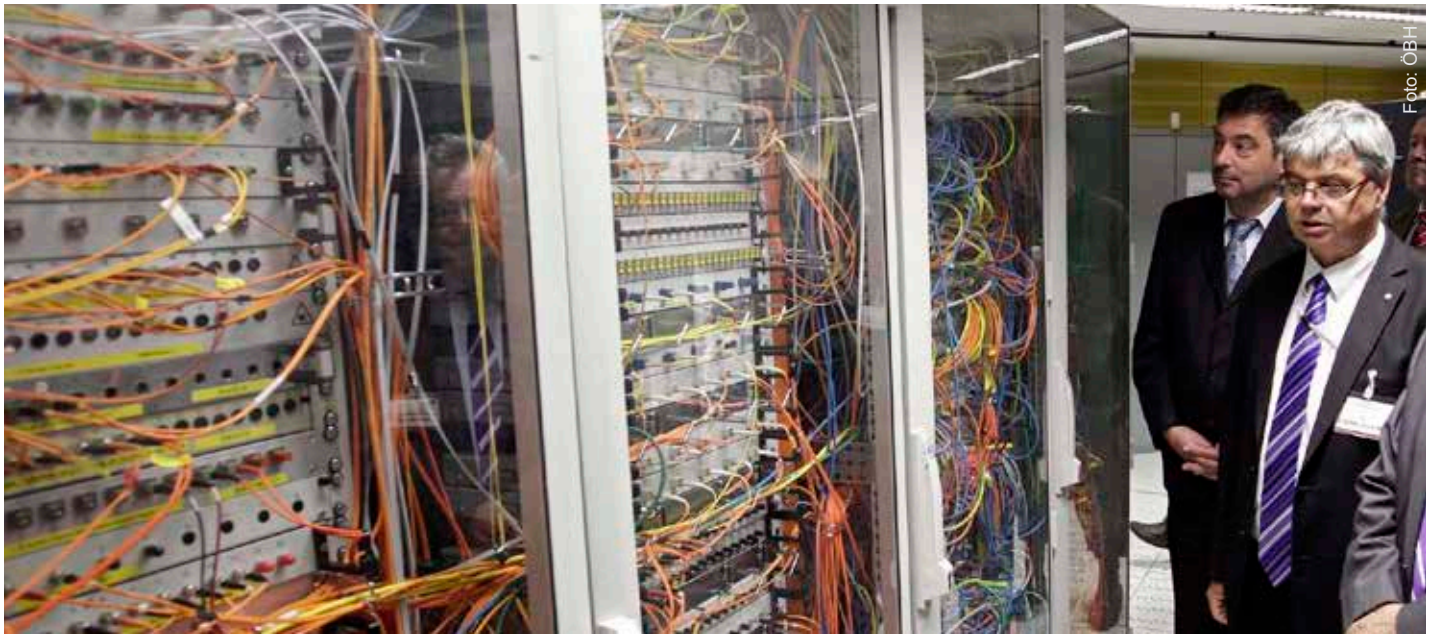
Foto: ÖBH

Bundesheergewerkschaft und AUF/AFH warnen seit Jahren

Bereits der Einführungsprozess wurde kritisch beobachtet und es wurde laufend öffentlich in unseren Fachzeitschriften und auch ressortintern in den entsprechenden Gremien der Personalvertretung im Zentralausschuss auf die verschiedenen Problembereiche der Sicherheit im neuen System hingewiesen. Bei der Einführung neuer Techniken und neuer Datenverarbeitungssysteme, die alle Bediensteten betreffen, ist die Personalvertretung zu befassen. Dies ist bislang nur mit einem Kurzvortrag und nicht im Rahmen einer ZA-Sitzung erfolgt. Somit liegt derzeit keine Zustimmung der Personalvertretung vor, das System OrgFlex einzuführen. Die Fraktion AUF/AFH hat nun für die kommende Sitzung im Zentralausschuss des BMLV einen entsprechenden Tagesordnungspunkt auf die Sitzungsagenda gebracht.

Sind alle Sicherheitsauflagen für einen Datentransfer erfüllt?

Für die Bundesheergewerkschaft stellt sich zudem die Frage, ob für die Verschlüsselung von Daten sensibler Dienststellen alle vorgeschriebenen Maßnahmen getroffen wurden. Eine Verschlüsselung alleine reicht nämlich nicht aus, um klassifizierte Informationen zu übermitteln. Die Verschlüsselung sollte durch die SAA (Akkreditierungsstelle Security Accreditation Authority bzw. durch die NCSA (National Communication Security Authority) im Bundeskanzleramt zugelassen sein. Für beteiligte externe Dienstleister muss für das Verteidigungsressort überdies eine Sicherheitsfreigabe bzw. Firmenprüfung des Heeresabwehramtes vorliegen.

Wem gehören die Daten der Soldaten und Bediensteten des BMLV?

Nicht klar geregelt scheint zu sein, wer letztlich der Besitzer der Personaldaten ist. Ist für die Datenverwaltung die Dienstbehörde, das Ressort oder die Republik Österreich zuständig? Die Bundesheergewerkschaft sieht hier den Bedarf einer juristischen Abklärung, weil man die Überlegung prüfen muss, ob dann zukünftig auch die EU-Behörden das Recht auf die Daten unserer Soldaten und Bediensteten haben werden. Die Bundesheergewerkschaft prüft dazu derzeit die Absicht eines Verfahrens zur rechtlichen Abklärung bis zum EuGH.

Bundesheergewerkschaft und AUF-AFH begrüßen Maßnahmen des IKT-Sicherheitsbeauftragten im BMLV

Es muss nun genauestens untersucht werden, ob alle Richtlinien der internen und externen Sicherheit im Bundesheer eingehalten worden sind. Aus gut informierten Kreisen wurde bekannt, dass sich nun auch der Datenschutzbeauftragte des Verteidigungsministers eingeschaltet hat und die gesetzlichen Voraussetzungen im Rahmen der EU-Datenschutzverordnung prüft. Die Bundesheergewerkschaft regt außerdem eine Revision des gesamten Projekts an, um erheben zu können, welche Kosten das Projekt Orgflex bis jetzt verursacht und wie das Projektmanagement die Einführung über die Jahre hin begleitet hat. Vor allem wäre es interessant zu erfahren, ob es Mehrkosten, Verzögerungen oder Probleme in der Umsetzung gegeben hat.

Für alle Personen, Unternehmen, Firmen und Konzerne gilt die Unschuldsvermutung.

Quellenverweise zu den öffentlichen Artikeln der FGÖ/BHG bzw. zum aktuellen IKT Sicherheitsvorfall im Innenministerium:

Datenvorfall BMI
September 2019
https://www.fass-ohne-boden.at/bmi-datenleck-programmierer-konnten-unbemerkt-auf-polizeidaten-zugreifen/

Bericht FGÖ-BHG
BigData 2017
https://www.yumpu.com/de/document/view/62848472/bigdataartikel2017

Bericht FGÖ-BHG
BigData 2016
https://www.yumpu.com/de/document/view/62848469/bigdataartikel-2016