Zeitschrift: Armee-Logistik : unabhängige Fachzeitschrift für Logistiker = Organo indipendente per logistica = Organ independenta per logistichers = Organ indépendent pour les logisticiens

Herausgeber: Schweizerischer Fourierverband

Band: 91 (2018)

Heft: 10

Rubrik: Herausgegriffen

ARMEE-LOGISTIK

91. Jahrgang. Erscheint 10-mal jährlich (monatlich, Doppelnummern 7/8 und 11/12).
ISSN 1423-7008.
Beglaubigte Auflage 3540 (WEMF 2016).

Offizielles Organ:
Schweizerischer Fourierverband (SFV) / Verband Schweizerischer Militärküchenchefs (VSMK) / Schweizerischer Feldweibelverband (SFwV)

Jährlicher Abonnementspreis: Für Sektionsmitglieder im Mitgliederbeitrag inbegriffen. Für nicht dem Verband angeschlossene Angehörige der Armee und übrige Abonnenten Fr. 32.–, Einzelnummer Fr. 3.80.
Postkonto 80-18 908-2

Verlag/Herausgeber: Schweizerischer Fourierverband, Zeitungskommission, Präsident Four Stefan Walder (sw), Aufdorfstrasse 193, 8708 Männedorf,
Telefon Privat: 079 346 76 70,
Telefon Geschäft: 044 752 35 35, Fax: 044 752 35 49,
E-Mail: swalder@bluewin.ch

Redaktion: Armee-Logistik, Sdt Florian Rudin (fr), Notariat Riesbach-Zürich, Postfach, 8034 Zürich,
Telefon Privat: 078 933 04 69,
Telefon Geschäft: 044 752 35 35, Fax: 044 752 35 49,
E-Mail: redaktion@armee-logistik.ch

Chefredaktor:
Oberst Roland Haudenschild (rh)
Sektionsnachrichtenredaktor: Sdt Florian Rudin (fr)
Mitarbeiter: Hartmut Schauer (Deutschland/Amerika). Oberst Heinrich Wirz (Bundeshaus/Mitglied EMPA);
Freier Mitarbeiter: Oberst i Gst Alois Schwarzenberger, E-Mail: schwarzenberger.alois@bluewin.ch,
Telefon 078 746 75 75

Redaktionsschluss:
Nr. 11/12 – 15.10.2018, Nr. 1 – 05.12.2018,
Nr. 2 – 05.01.2019
Grundsätzlich immer am 5. des Monats für die Ausgabe des kommenden Monats.

Adress- und Gradänderungen:
SFV und freie Abonnenten:
Zentrale Mutationsstelle SFV, Postfach,
5036 Oberentfelden, Telefon 062 723 80 53,
E-Mail: mut@fourier.ch

VSMK-Mitglieder: Verband Schweizerischer Militärküchenchefs, Zentrale Mutationsstelle VSMK,
8524 Uesslingen, mutationen.vsmk@bluewin.ch

Inserate: Anzeigenverwaltung Armee-Logistik,
Sdt Florian Rudin, Notariat Riesbach-Zürich, Postfach,
8034 Zürich, Telefon Geschäft: 044 752 35 35
(Hr. Walder), Fax: 044 752 35 49,
E-Mail: swalder@bluewin.ch
Inseratenschluss: am 1. des Vormonats

Druck: Triner Media + Print, Schmiedgasse 7, 6431 Schwyz, Telefon 041 819 08 10, Fax 041 819 08 53

Satz: Triner Media + Print

Vertrieb/Beilagen: Schär Druckverarbeitung AG, Industriestrasse 14, 4806 Wikon,
Telefon 062 785 10 30, Fax 062 785 10 33

Schutz vor Cyber-Angriffen

Grundlage für die Strategie und die Massnahmen des VBS zum Schutz vor Cyber-Angriffen ist die Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS). Sie hat zum Ziel, in Zusammenarbeit zwischen Behörden, Wirtschaft, Hochschulen und den Betreibern kritischer Infrastrukturen die Cyber-Risiken zu minimieren.

Die NCS 2012–2017 umfasst 16 Massnahmen. Am 18. April 2018 verabschiedete der Bundesrat die NCS 2018–2023. Diese baut auf den Arbeiten der ersten NCS auf, weitet diese wo nötig aus und ergänzt sie mit neuen Massnahmen.

Nachrichtendienst des Bundes: Melde- und Analysestelle

Die Melde- und Analysestelle Informationssicherung (MELANI) und ihre Aufgaben ist in Armee-Logistik Nr. 3, März 2018, S. 1, ausführlich beschrieben.

Armee: Fokus auf Schutz eigener Infrastrukturen

Die Armee spielt in den Vorkehrungen zum Schutz vor Cyber-Risiken eine wesentliche Rolle. Sie stützt sich, wie die gesamte Gesellschaft, stark auf Informations- und Kommunikationstechnologien ab und kann das Ziel von Cyber-Angriffen sein. Deshalb muss sie zunächst ihre eigenen Infrastrukturen und Mittel schützen. Sie investiert in Netze, die gegenüber Angriffen und Gefahren aller Art geschützt sind. Dazu zählen die Projekte zum Neubau von Rechenzentren, Telekommunikation der Armee und Führungsnetz Schweiz.

Soweit die Armee ihre eigenen Schutzbedürfnisse erfüllt hat, kann sie bei Bedarf ihre Kapazitäten zum Schutz vor Cyber-Angriffen subsidiär zivilen Behörden zur Verfügung stellen und damit einen Beitrag zur Aufrechterhaltung der Funktionsfähigkeit der kritischen Infrastruktur leisten.

Im Fall eines bewaffneten Konflikts würde die Armee alle ihre Fähigkeiten im Cyber-Bereich einsetzen, um Angriffe zu verhindern, ihre Wirkung zu vermindern und gegnerische Fähigkeiten in diesem Bereich zu schwächen.

Bundesamt für Bevölkerungsschutz: Risiko- und Verwundbarkeitsanalysen

Aufgabe des BABS ist es, die Bevölkerung und ihre Lebensgrundlagen bei Katastrophen und in Notlagen sowie im Falle bewaffneter Konflikte zu schützen und so wesentlich zur Begrenzung und Bewältigung von Schadenereignissen beizutragen. Es führt im Rahmen der NCS Risiko- und Verwundbarkeitsanalysen für kritische Infrastrukturen durch. Basierend auf diesen Analysen erarbeitet das BABS zusammen mit den Regulierungsbehörden, Verbänden und Betreibern kritischer Infrastrukturen (Spitäler usw.) Massnahmen zur Reduktion der Risiken.

Die zivilen Behörden sind darauf angewiesen, dass ihre Telekommunikations- und Alarmierungssysteme in allen Lagen funktionieren und dass die Bevölkerung über gesicherte Kanäle gewarnt und alarmiert werden kann sowie mit verlässlichen Informationen versorgt wird. Das BABS beschäftigt sich auf Ebene Bund mit mehreren Projekten für krisen- und stromsichere Kommunikationsnetze.

Informations- und Objektsicherheit des VBS

Im VBS ist die im Generalsekretariat angesiedelte Informations- und Objektsicherheit (IOS) für den Schutz vor Cyber-Angriffen verantwortlich. Die IOS betreut die integrale Sicherheit des VBS. Sie ist insbesondere für die Vorgaben im Bereich der Sicherheit von Personen, Informationen, Informatik und Sachwerten (Material und Immobilien) zuständig.

Aktionsplan Cyber-Defence des VBS

Mit der Intensivierung der Cyber-Risiken, Erfahrungen mit konkreten Angriffen und neuen Rechtsgrundlagen beschloss der Chef VBS 2016, das VBS-Dispositiv zum Schutz vor Cyber-Angriffen zu überprüfen. Daraus entstand ein Aktionsplan Cyber-Defence, der bis 2020 umgesetzt werden soll. Die Umsetzung des Aktionsplanes wird im Einklang mit der übergeordneten nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken erfolgen.

Auch der Bund intensiviert seine Anstrengungen bei der Prävention und der Bekämpfung von Cyber-Risiken. Im Hinblick auf den Aufbau eines entsprechenden Kompetenzzentrums hat der Bundesrat an seiner Sitzung vom 4. Juli 2018 erste Grundsatzentscheide gefällt und verschiedene Aufträge erteilt. Definitiv entscheiden wird er Ende 2018.

Quelle: www.vbs.admin.ch

(rh)