Facebook-Knigge für Soldaten

Nach Armee-Skandalen in den sozialen Medien fordern Sicherheitspolitiker klare Richtlinien

Roland Gamp

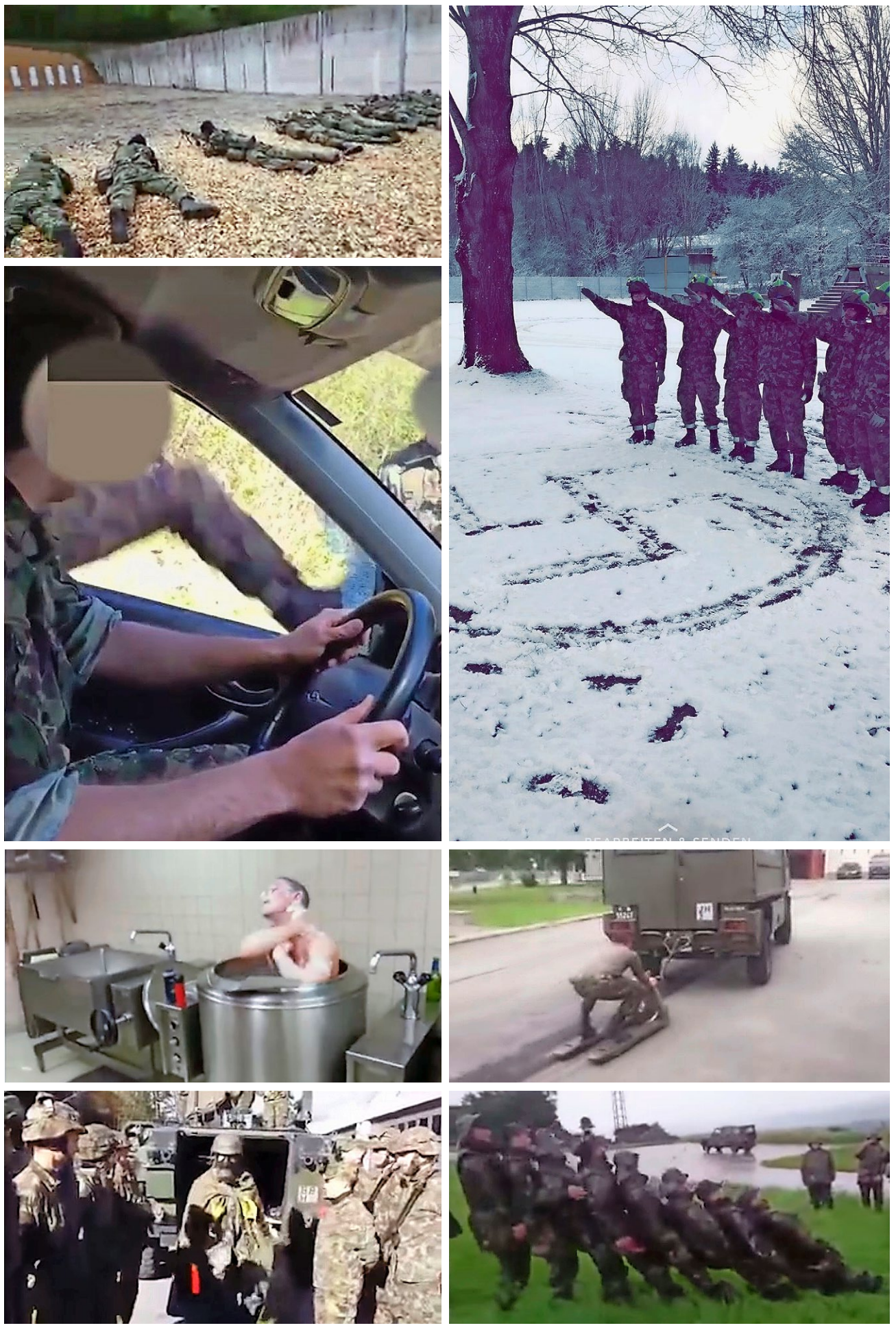
Bern Die Soldaten der «besten Armee der Welt» beschäftigen die Militärjustiz intensiv. 300 Beweisaufnahmen hat sie 2016 eröffnet – so viele wie noch nie seit der Jahrtausendwende. Damals zählte das Korps allerdings noch doppelt so viele Angehörige.

Die Strafverfolger untersuchten die Affäre um Oberfeldarzt Stettbacher, den tödlichen Unfall eines F/A-18-Piloten am Sustenpass oder die Beschaffung des Bodluv-Systems. Meist jedoch handelte es sich um Fälle von geringerer Tragweite. Laut Statistik waren die meisten Delikte 2016 einfache «Dienstversäumnisse». Dahinter folgten «Nichtbefolgung einer Dienstvorschrift», «Missbrauch und Verschleuderung von Material» und die Rubrik «Strassenverkehrsgesetz». Juristisch gesehen also oft Bagatellen. Doch diese finden zunehmend den Weg an eine breite Öffentlichkeit. Und setzen dem Image der Armee so arg zu.

Hakenkreuz, Gewaltaufruf und ein demoliertes Auto

Letzte Woche sorgte ein Uniformierter für Schlagzeilen, der aggressiv ein Auto demolierte. Im April forderte ein Vorgesetzter Rekruten auf, auf die Freundin zu schiessen, wenn diese untreu sei. Im Januar posierten Rekruten auf einem Waffenplatz mit Hakenkreuz und Hitler-Gruss. Alle Vorfälle wurden mit dem Smartphone festgehalten. Die entsprechenden Filme und Bilder fanden ihren Weg auf die sozialen Netzwerke. Und dort Hunderttausende Zuschauer. Ein neunminütiges «Best of»-Video von herumblödelnden Soldaten etwa erreichte über eine halbe Million Views auf Youtube.

Das ärgert Sicherheitspolitiker aller Lager. Nationalrat Hans Fehr (SVP): «Unsere Bevölkerung stellt sich bei einer Zunahme solcher Vorkommnisse zu Recht die Frage, ob eine solche Armee etwas taugt und ob sie ihren Auftrag überhaupt erfüllen kann.» Der Oberstleutnant, selbst leistete er rund 1400 Diensttage, sieht mehrere mögliche Gründe: «Ein langweiliger Dienstbetrieb, keine klaren Aufträge, fehlende Kontrollen, keine oder keine wirksamen Sanktionen bei Verstössen.» Fehr nimmt die Führungsriege in die Verantwortung: «Die Vorgesetzten müssen für einen anspruchsvollen und straffen Dienstbetrieb sorgen, klare Forderungen bezüglich Disziplin, Kleidung und Auftreten stellen und diese auch durchsetzen.»



Die Videos und Fotos finden Hunderttausende Zuschauer in den sozialen Medien und schaden so dem Image der «besten Armee der Welt»: Armeeangehörige inszenieren sich als Neonazis, Frauenhasser oder einfach als Witzbolde

Auch Corina Eichenberger (FDP), Präsidentin der Sicherheitskommission des Nationalrats, ist verärgert: «Solche Fälle lösen jedes Mal einen Image-Schaden aus.» Jugendliche würden immer leichtfertiger mit sozialen Medien umgehen, auch in der Armee. Es brauche deshalb mehr Aufklärung durch die Vorgesetzten. «Sie müssen die Konsequenzen besser aufzeigen. Und klarmachen, dass solche Videos ein schlechtes Licht auf die gesamte Armee werfen», so Eichenberger. Sie fordert Richtlinien für Militärangehörige im Umgang mit sozialen Medien.

«Die Hemmschwelle, etwas ins Netz zu stellen, sinkt»

Edith Graf-Litscher (SP), ebenfalls Mitglied der Sicherheitskommission, schliesst sich an: «Viele Unternehmen haben heute Richtlinien, wie Angestellte mit Social Media umgehen sollen», sagt die Nationalrätin. «Solche Richtlinien müsste auch die Armee ausarbeiten.» Zudem wären Schulungen sinnvoll. «Die Rekruten lernen bei der Armee enorm viel. Die Nutzung neuer Medien sollte dazugehören.»

Aus Sicht der Armee sind nicht alle Zwischenfälle gleich problematisch: «Wenn jemand ein Auto zertrümmert, ist das eine Bagatelle, die man disziplinarisch abhandeln kann», sagt Daniel Reist, Kommunikationschef Verteidigung. «Fälle von Rassismus oder Sexismus hingegen melden wir konsequent bei der Militärjustiz.» Einen grundsätzlichen Rückgang der Disziplin habe man nicht festgestellt. «Aber die Hemmschwelle, etwas ins Netz zu stellen, sinkt.» Der Dienstbefehl hält schon heute fest, dass Video-, Bild- und Tonaufnahmen nur mit ausdrücklicher Erlaubnis des Kommandanten erlaubt sind. «Wer sich nicht daran hält, wird abgemahnt», sagt Reist.

2012 erarbeitete die Armee zudem ein «Social Media Handbuch». Es richtet sich aber vor allem an Kommunikationsspezialisten im Korps. Richtlinien für jeden Armeeangehörigen sind laut Reist unrealistisch. «Wir sprechen von 190 000 Personen, viele von ihnen sind nur drei Wochen im Jahr anwesend. Es wäre logistisch kaum umsetzbar, jeden von ihnen mit solchen Richtlinien zu erreichen.»

IT-Bericht stellt Sicherheitslücke bei Sunrise fest

Hacker konnten die Internet-Telefonie des Telecom-Anbieters leicht angreifen. Man habe das Problem «innert kürzester Zeit» behoben, sagt die Firma

Zürich Die Internet-Telefonie ist nicht sicher. Das ist in der IT-Branche ein ungeschriebenes Gesetz. Besonders Gratisangebote wie Skype oder Whatsapp sind den Sicherheitsexperten ein Dorn im Auge. Sie warnen davor, auf diesen Kanälen sensible Daten wie Passwörter oder AHV-Nummern auszutauschen. Hacker könnten mitlesen und -hören.

Dasselbe gilt offenbar auch für die Internet-Telefon-Angebote von Schweizer Anbietern, vor allem von Sunrise. Das geht aus dem «Swiss Vulnerability Report» der Churer Sicherheitsfirma First Security Technology (FST) hervor, der kommenden Mittwoch erscheinen wird. Betroffen sind gegen 135 000 Privatkunden, KMU und teilweise auch Grossunternehmen.

Für den Internetempfang zu Hause oder im Unternehmen ist ein Router nötig. Die FST hat bei einem gross angelegten Test des Schweizer Internets 138 000 offene Router-Ports gefunden, die für Internettelefonie benutzt werden. Ports sind Kanäle, über die mit anderen Rechnern oder Programmen im Internet kommuniziert wird. Auf offene Ports kann von Hackern direkt zugegriffen werden, um etwa Gespräche mitzulauschen. 135 000 dieser Ports gehören Geräten der Marke Fritzbox, die von Sunrise eingesetzt wird.

Der Bericht abschliessend: «Wir gehen davon aus und hoffen, dass dieser Internet-Service-Provider sich dieses Risikos bewusst ist und diesen Dienst beobachtet und daher entsprechende Sicherheitsvorkehrungen getroffen wurden.» Eine ähnliche Sicherheitslücke bei der Deutschen Telekom wurde letztes Jahr von Hackern ausgenutzt, um Passwörter oder Kreditkartennummern zu stehlen.

FDP-Nationalrat fordert: KMU müssen Security auslagern

Man habe die Sicherheitslücke Anfang Jahr mit einem Update geschlossen, heisst es bei Sunrise. «Die genannte Kritik ist daher nicht mehr gerechtfertigt», sagt Sprecher Rolf Ziebold. Genauere Angaben, etwa wie lange die Lücke bestand, wollte Sunrise nicht machen. Der Telekom-Anbieter sagt: «Sunrise schloss die Sicherheitslücke innert kürzester Zeit, nachdem wir vom Hersteller die entsprechende Information erhalten hatten.» Pascal Mittner, CEO der First Security, sagt: «Dass Sunrise schnell reagiert hat, ist gut. Noch besser wäre es, den Port ganz vom offenen Internet zu nehmen.» Man würde Hackern so nur eine unnötige Angriffsfläche bieten.

Auch KMU müssen sich verstärkt auf Cyber-Angriffe einstellen. Deren IT-Abteilungen könnten die zunehmend raffinierten Hacker-Angriffe nicht mehr abwehren, sagt FDP-Nationalrat und Digitec-Co-Gründer Marcel Dobler. Er fordert: «KMU müssen vermehrt die Sicherheit an externe Firmen vergeben.»

Für den Bericht wurden alle 20 Millionen Schweizer IP-Adressen abgegrast. Diese Adresse ist die Identitätskarte des Computers im Internet: Er zeigt, dass schweizweit 36 000 Datenbanken, 7300 Drucker und 3800 Webcams offen im Internet zugänglich sind. Mit ein paar Programmiertricks können Hacker direkt in die Wohn- und Schlafzimmer von Herr und Frau Schweizer blicken. **Wissen — 50**

Barnaby Skinner, Simon Widmer