Bundeswehr: Die Vertuschung als neustes Mittel der IT-Security

---

Wenn uns im Rahmen der Digitalisierung die rosaroten Wolken verkauft werden, werden uns gern die Prämissen unterschlagen. Nötige Netzbandbreiten, Hochverfügbarkeit, Sicherheitsanforderungen und vor allem auch Risiken. Es hat immer alles rosarot zu sein. Weil nur diese Farbe für besser steht.

Da zumindest einige bei der Bundeswehr erkannt haben, dass viel Licht auch viel Schatten wirft, war man so umsichtig mit dem neuen Kommando CIR (Cyber- und Informationsräume) eben diesen Risiken besser begegnen zu können. Und natürlich auch, um selbst Optionen im Kampf von Bits gegen Bytes zu haben. Technisch wie finanziell gesehen trifft dieser Satz sogar die faktische Realität. Man kämpft ohnehin ausstattungsmäßig im Mittelfeld dessen, was man als Bedrohung ausgemacht hat. Quasi sabbernd am Spielfeldrand stehend. Als Reserveersatzreserve der Mainplayer.

Und damit nicht genug, denn dann wurde populistisch und vor allem pressewirksam das neue „Bundeswehr-Space-Kommando“ zusätzlich in Szene gesetzt. Zwar nicht ganz so schön, wie das US-Space-Command, das sogar das Raumschiff Enterprise Emblem zu seinem Wappen gemacht hat, aber immerhin schon mal dem Namen nach. Und folgerichtig in einer runtergekommenen Kaserne untergebracht, damit Anspruch und Anschein schon mal optisch die Waage finden…

Doch warum so hoch hinaus, wenn es schon auf der simpelsten Ebene nicht funktioniert? Der DAU (dümmster anzunehmender User) wieder zugeschlagen hat und alle Prozesse, Regularien, Vorschriften und verbindliche Meldewege versagen? Deshalb versagen, weil opportunistischer Eigennutz zum individuellen Karriereerhalt doch höherwertiger zu betrachten ist, als der Anspruch der Bundeswehr und der Bundesrepublik Deutschland auf sichere Cyber- und Informationsräume. Egal ob weltraumgestützt (hüstel…) oder bodengebunden 1.0 und „verdrahtet“.

Und wieder kommt hier der Standort Pfullendorf und das Ausbildungskommando Heer in Leipzig ins Spiel. „*Heer sein, heißt mehr sein*“, wurde uns damals in den 80iger Jahren eingeimpft. Und so war es klar, dass gerade auch das Ausbildungskommando Heer als Vorreiter der Ausbildung beim Heer seine ureigenen DAUs zahlreich heranzüchten konnte. Neben anderen Experten und Kompetenzträgern zu Themen wie sexuelle Belästigung, Rechtsextremismus und weiteren Feldern medienwirksamer Vorteilhaftigkeit. Das war böse, zeigt aber die Tendenz.

Doch nun zum Fall an sich, ein Fall, der jedes zivilwirtschaftliche Unternehmen, jede Behörde und auch jede andere Dienststelle hätte treffen können. Vermutlich sogar viele schon getroffen hat, die es aber noch gar nicht wissen.

Ein schönes Beispiel für gut gemeint, viel gewollt, wenig

gewusst und daher blöd gelaufen.

Anstatt nun glücklich zu sein, dass durch die rechtzeitige und proaktive Eigeninitiative einiger weniger der Schaden überschaubar gewesen wäre, wurden nun diejenigen, denen es aufgefallen ist, verfolgt.

Exakt aus diesem Grunde hat die Bundeswehr auch Meldewege für IT-Sicherheitsverstöße so implementiert, dass Meldungen über Sicherheitsvorfälle auch auf anderen Meldewegen zur Kenntnis nächstverantwortlicher Dienststellen gelangen können. Abseits der normalen sog. dienstlichen Meldewege. Eben damit der Faktor Mensch und sein „individuelles Karriere- und Schutzbedürfnis“ hinter der Sicherheit für alle zurückstehen. Somit theoretisch hervorragend ausgedacht. Theoretisch. Aber wie sieht die Praxis aus?

Eigentlich so, wie wir es auch für Corona in der Pandemie anstreben. Und offene Netzzugänge und Datenzugriffe wirken genauso pandemisch, wie Covid-19. Daher haben viele Fachbegriffe in der IT-Security auch biologische Vettern aus der Virologie.

Oberstleutnant L., Chef der IV. Inspektion am Ausbildungszentrum, wollte im Lockdown via Homeoffice die Möglichkeit schaffen Übungslagen (Szenarien um den Militäreinsatz zu üben) zu bearbeiten bzw. bearbeiten zu lassen. Nur war, welch Wunder, die Bundeswehr dafür nicht ausgerüstet. Ähnlich wie die Schulen, wo Kinder von jetzt auf gleich digital beschult werden sollten und viele Lehrkräfte erst einmal den Umgang mit dem Internet lernen mussten. Also kein Einzelfall. Nur nutzte der besagte Oberstleutnant nicht dafür zertifizierte und somit auch nicht genehmigte Mittel: einen NAS (Datenspeicher mit eigenem Betriebssystem der an ein Netz angeschlossen ist, Network Attached Storage)! Einen

Datenspeicher mit prinzipiell offenen und ungeschützten Leitungen mit der Zugriffsmöglichkeit von außen. Für eine militärische Anwendung…
Die beauftragten Soldaten sollten schließlich von ihrem Homeoffice über diesen Speicher, angeschlossen auf das private Notebook in der Privatwohnung des Vorgesetzten zugreifen können. Ein „Schutz“ einfachster Art wurde implementiert. Der Offizier hätte das Ganze im Endeffekt auch via Facebook-Gruppe starten können…

Es ging hierbei unter anderem um Übungslagen und Vorschriften für Recovery-Operationen. Das sind militärische und sehr riskante Operationen, die immer dann anlaufen, wenn beispielsweise Luftfahrzeugbesatzungen hinter den feindlichen Linien abgeschossen werden und zurückgeholt werden müssen. Wie im Film *Bat-21* mit Gene Hackman.

Es gibt dafür spezifische Handlungsweisen, die von zu Rettenden wie auch durch die Retter regelmäßig zu üben sind. Diese sind meist NATO-einheitlich, damit jede Nation auch Soldaten anderer Nationen retten kann und diese das Procedere umfänglich genug kennen, um nicht sich und die Retter zu gefährden. Kennt der Feind diese Abläufe, kann er diese dazu verwenden um den/die zu Rettenden wie einen Köder für den Fisch zu nutzen und das Recovery-Team in eine Falle zu locken.

Das wurde so in Afghanistan, Vietnam und anderswo immer wieder gern gemacht.

Und eine solche Lageübung mit dem entsprechenden Procedere, Einstufung VS-NfD, hat nun Oberstleutnant L. den Übungsteilnehmern auf einem Speicher präsentiert. Einem Speicher, der jedem via Internet Zugriff ermöglichte, wenn er nur die denkbar simpelsten Zugriffsmöglichkeiten kannte. Hier geht es nicht nur um den Geheimhaltungsgrad, der ist denkbar niedrig gehalten, damit man damit überhaupt üben kann, sondern um das Thema(!) der Übung und Durchführung an sich. Die mögliche Missionsgefährdung von Recovery-Operationen im

Einsatz.

Schon bei der Einrichtung dieses Netzwerkspeichers bemerkten zwei aufmerksame Feldwebel, dass hier ein massiver Verstoß gegen interne IT-Security-Richtlinien vorlag und suchten das Gespräch mit Herrn L. Sie hätten diesen Vorgang auch gleich an die IT-Abteilung des Standorts melden können. Sogar müssen!

Doch anstatt den Fehler einzusehen und um Hilfe zu bitten „die Nummer noch aus dem Dreck zu ziehen“, wurden die beiden Feldwebel zum Schweigen verdonnert. Für solche Fälle hat die Bundeswehr jedoch Regularien geschaffen, um EXAKT so etwas zu verhindern!

Beide Unteroffiziere meldeten pflichtbewusst und vorschriftengemäß dem S6 Offizier (Fernmelde- und IT-Offizier), der wiederum einen Bericht für den Kommandeur des Ausbildungszentrums in Pfullendorf erstellte. Dieser, Oberst KK, gab den Fall wohl an seinen Stellvertreter Oberstleutnant L1 weiter, zumal dieser in einem ähnlichen Fall einen Reserveoffizier vor das Truppendienstgericht brachte. Und dieser Oberstleutnant L1 hat nun was getan? – Genau: NICHTS! Besser noch, er wiegelte den Bericht des S6 Offiziers wegen „nicht zutreffend“ ab.

Gleichzeitig wurde gegen einen der Feldwebel wegen „Gehorsamsverweigerung“ disziplinar ermittelt. Beide Feldwebel erhielten eine Disziplinarstrafe da sie sich angeblich nicht an den Dienstweg gehalten hätten.

Ab solchen Zeitpunkten kocht es dann in Truppenverbänden. Ungerechtigkeit zeigt Wirkung und der Fall fiel bildlich gesehen über den Kasernenzaun. Über zwei Zwischenstationen kam er zum Autor, der dann ein paar Telefonate führte. Ja, in Pfullendorf herrschte nun Friedhofsruhe. Der örtliche Personalrat tagte, Soldaten, auch weibliche, suchten Ärzte aufgrund psychischer Belastungen auf. Das Wort Mobbing hing in der Luft und auch die Vorzimmerdame von Oberstleutnant L., dem

Verursacher der Krise, fühlte sich zunehmend unwohl.

Wie wir alle wissen, kommen Kompetenz und gutes Führungsvermögen bei Menschen gern gleichzeitig vor. Und so trieb das, was zusammengehört, neue Blüten.

Der Autor entschloss sich also zu einer Presseanfrage mit dem expliziten Hinweis auf eine heutige Veröffentlichung. Einmal an den Presseoffizier in Pfullendorf (dies ist dort der Personaloffizier in Personalunion) mit Fragen an den Kommandeur Oberst KK gerichtet. Und dann in etwas genauerer Form, mit Details gespickt, an den stv. Kommandeur CIR, Generalmajor Setzer, der der höchstrangige IT-Sicherheitsbeauftragte der Bundeswehr ist. Dabei wurde der IT-Sicherheitsbeauftragte des Heeres bewusst übersprungen.

Es kam, wie es kommen musste. General Setzer witterte die Bärenfalle und ließ via Presseoffizier CIR mitteilen:
„Die Fragen betreffen mehrere unterschiedliche Themen und Zuständigkeiten. Um die Fragen beantworten zu können, bedarf es erst einmal der Prüfung einiger Rahmenbedingungen, die in truppendienstlicher Zuständigkeit liegen. Vor diesem Hintergrund bitten wir darum sich mit diesem Anliegen an das Kommando Heer, Presse- und Informationszentrum des Heeres, zu wenden.“

Das Pressezentrum CIR funktioniert vorbildlich. Und ist aus Sicht des Autors eine pressetechnische Vorzeigestelle der Bundeswehr. Somit schuf sich das CIR die Möglichkeit als letztmögliche Meldestelle innerhalb der Bundeswehr selbst noch einen Daumen auf der Sache zu haben, um gegebenenfalls noch „Anpassungen“ vorzunehmen zu können.

Natürlich wurde das Heer nicht befragt, da der Autor aus Erfahrung weiß, dass nun der „kleine Dienstweg“ anlief und die Verantwortlichen mit bei der Bundeswehr so beliebten bcc-Verteilern (nicht sichtbare parallele Weiterleitung von Mails an andere Empfänger) vorab informiert wurden, dass „da etwas

im Busch ist“.

Dass sich der Kommandeur in Pfullendorf nicht meldete war vorhersehbar gewesen. Nur wusste weder Pfullendorf noch das CIR von der jeweiligen anderen Presseanfrage.

Inzwischen war einem der Feldwebel in Pfullendorf klar geworden, dass das Melden am Vorgesetzten vorbei parallel an die nächsthöhere Ebene vorschriftenkonform war. Er schilderte den gut dokumentierten Fall schriftlich beim IT-Sicherheitsbeauftragten des Kommandos Heer in Strausberg. Hierüber erhielt er sogar eine Eingangsbestätigung. Auf telefonische Nachfrage wurde ihm mitgeteilt, dass der Vorgang seiner Meldung an das Ausbildungskommando in Leipzig weitergeleitet wurde und diese sich dann wiederum mit der untergeordneten Dienststelle in Pfullendorf abstimmen würden, da ja eigentlich der Kommandeur in Pfullendorf diesen schwerwiegenden Sicherheitsverstoß melden müsste. – Oder hätte melden müssen…

Und das hat Pfullendorf bis dato nicht getan. Doch was man in Pfullendorf nicht weiß, ist der Umstand, dass man höheren Orts schon von dem Vorfall explizit informiert wurde. Auch darüber, dass Pfullendorf hier einen gravierenden IT-Sicherheitsvorfall nicht gemeldet hat. Und auch, dass die Zeit abläuft. Abgelaufen ist. – Klappe zu, Affe tot!

Wie das Drama nun weitergeht, mag die Zukunft erweisen. Fest steht, dass das schönste Versprechen mehr leisten zu wollen, auf der „Schlammebene“ scheitert, wenn man nicht auch dafür sorgt, dass ein Gefühl für IT-Sicherheit vorhanden ist. Nicht als Lippenbekenntnis, sondern ganz real bei der Arbeit.

Jeder macht Fehler. Dies hat der Autor auch in seiner aktiven Zeit als Offizier erfahren. Und wenn es eng wurde, dann sagt man, dass man A) Mist gebaut hat und bittet B) um Hilfe. Diese wurde nie verwehrt. Der „Blödsinn“ bereinigt, begradigt und/oder auf die richtige Bahn gebracht und am Ende zahlte man

das Bier für den gemeinsamen „Du-Idiot-Abend“. Nach dem abschließendem Anschiss beim Chef/Kommandeur, der auch ein Bier abbekam. Dies wird auch gelegentlich als Kameradschaft bezeichnet.

Der Fall in Pfullendorf hätte so nicht hochkochen müssen. Es ist auch nicht der einzige Vorfall. Man hätte das bereinigen können. Schnell und sauber. Einen Bericht schreiben, dass man *kurzzeitig* so etwas eingerichtet hatte aber *rechtzeitig* erkannt hat, dass es so nicht geht und *proaktiv* dennoch melden wolle. Um einen möglichen aber unwahrscheinlichen Schaden abzuwenden. – Nichts wäre passiert! Gar nichts!

Stattdessen wurden und werden zwei aufmerksame Feldwebel drangsaliert, Berichte geradegebogen, Meldewege aktiv blockiert und der Bundeswehr Schaden zugefügt

Und im Einsatz, abgeschnitten und allein im Dreck hockend, die Häscher auf den Fersen, wird es sich nun jeder Soldat überlegen, ob er um Hilfe ruft und riskiert, dass die Kameraden des Recovery-Teams seinetwegen in einen Hinterhalt geraten. Man doch lieber auf eigene Faust versucht die eigene Truppe wieder zu erreichen. Trotz aller absolut gegenteiligen Chancen.

Dummheit passiert. Kann jedoch durch Kameradschaft „aufgefangen“ werden. Aber bornierte Arroganz mit Machtdenken ist jenseits dessen, was man noch als DAU definieren könnte. Es ist schlicht das Grab für jedes Netz, für jede Datenbank und für jedes Bestreben die kritischen IT-Verbindungen abzusichern.

Anstatt also ein „Enterprise-Kommando“ pressewirksam ins Leben zu rufen, sollte die Ministerin Pfullendorf neu bewerten und dort endlich für die Art von zukunftsweisender Professionalität sorgen, die das Heer in der Ausbildung braucht. Auch in der digitalen Ausbildung.

Wie inzwischen allgemein bekannt ist kann Homeoffice und Onlinelernen sogar Kosten sparen. Gelder freimachen. Für dringend benötigtes Gerät.

Und immer daran denken: Vertuschung löst keine Probleme! Schafft aber jede Menge neue… **sic**!
