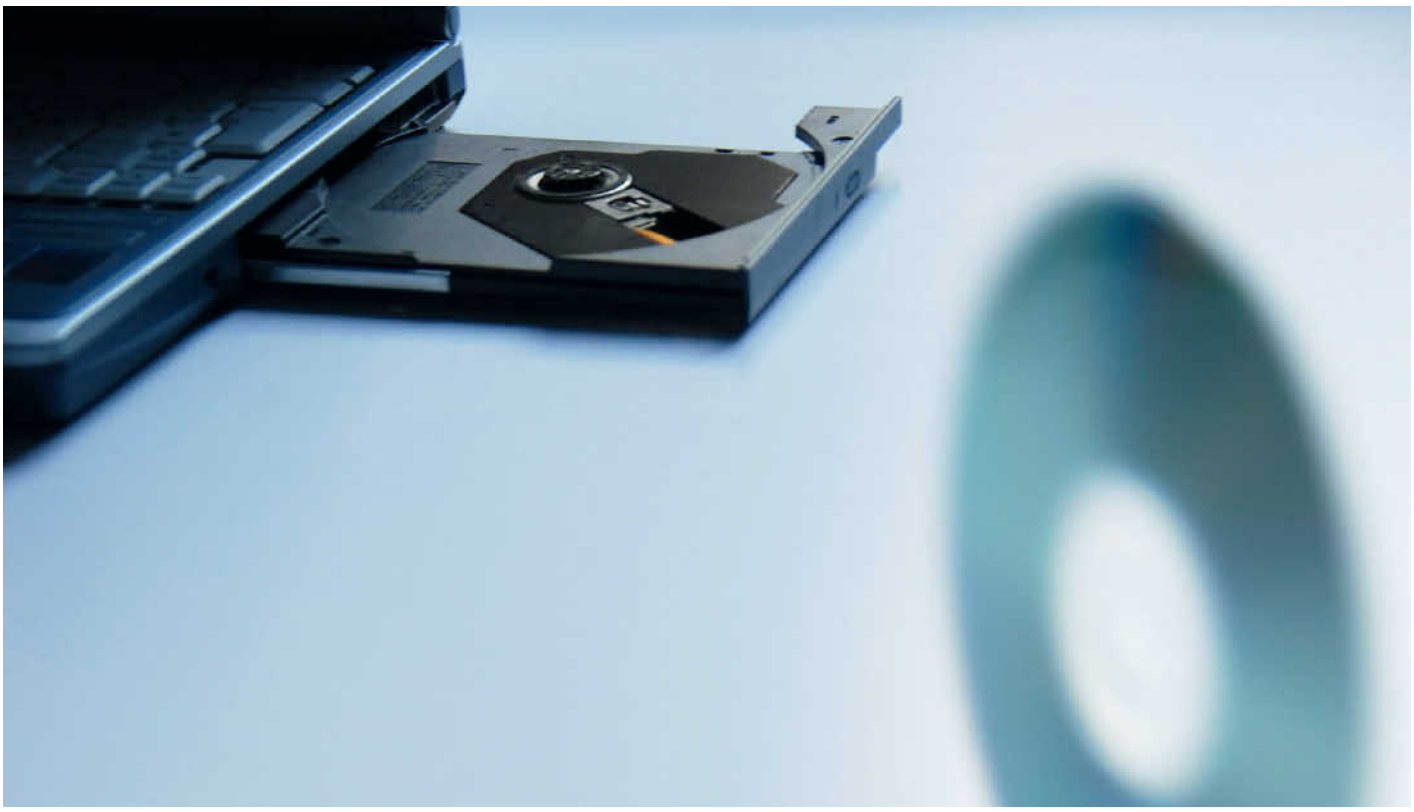

Datenklau beim NDB – lässt sich der Human Factor kontrollieren?

Im Mai 2012 wurde beim Schweizer Nachrichtendienst (NDB) ein Datenleck entdeckt. Ein IT-Mitarbeiter kopierte Terabyte-weise Daten. Nur durch Zufall wurde der Datenklau entdeckt. Wenn schon der NDB Probleme mit der Sicherheit der Daten hat – da fragt sich manch einer, was er in seinem Betrieb noch tun kann.

Von Richard Werner, Gabriela Suter

Am 25. Mai 2012 um 22.30 Uhr verhaftet die Bundespolizei einen IT-Mitarbeiter des Schweizer Nachrichtendienstes (NDB). Dieser hatte innert kurzer Zeit mehrere Gigabytes streng vertraulicher Daten von den Geheimdienstservern heruntergeladen, auf Festplatten gespeichert und sie zu Hause zum weiteren Verkauf hinterlegt. Dank einem aufmerksamen UBS-Kundenberater ist der Spionageanschlag aufgeflogen, bevor Schlimmeres geschehen konnte: Als Vorbereitung für den Verkauf wollte der NDB-Mitarbeiter bei der UBS ein Nummernkonto eröffnen. Beim Gespräch mit dem IT-Spezialisten wurde der Kundenberater misstrauisch und machte aufgrund des Geldwäschereigesetzes Meldung. Der Rest ist bekannt: Nach der Rückmeldung zum NDB konnte der Sachverhalt umgehend sichergestellt werden, und es kam zur Verhaftung.

Zweifelsfrei bestehen beim Nachrichtendienst besonders strenge Sicherheitsmassnahmen, die internationalen Standards entsprechen – trotzdem kam es zum Informations-GAU mit dem Diebstahl. Selbst wenn noch keine Daten weitergegeben wurden und kein Informationsleck entstanden ist, sprechen Insider von einem Vertrauensverlust, der dem NDB bei anderen Nachrichtendiensten entstanden ist. Der muss wieder mit mühsamer Kleinarbeit erarbeitet werden und könnte bedeuten, dass andere Geheimdienste vorab mit dem Datenaustausch zurückhaltend sind. Daten sind das Kerngeschäft eines jeden Nachrichtendienstes – der NDB könnte somit in seiner Hauptaufgabe für einige Zeit geschwächt sein.

«Leitfaden für die nächste Katastrophe»

Der IT-Spezialist des NDB war mit seinen Arbeitsbedingungen unzufrieden, das Unvermögen, mit seinem Umfeld klarzukommen, führte ihn zur Straftat. Die Geschichte könnte dem «Leitfaden für die nächste Katastrophe» von Charles Perrow entnommen sein. Bereits vor 20 Jahren formulierte er sechs Punkte in Organisationen, die zum GAU führen können. Die Aufzählung von Perrow beschreibt gefährdete Organisationen.

Was für den Nachrichtendienst die Daten über Terrorismus, Satellitenüberwachung, beschattete Personen etc. sind,

sind für Betriebe Unterlagen aus dem Geschäftsalltag, Kundendaten, Prozessbeschreibungen, Konstruktionspläne, Unterlagen zur Strategie oder Kennzahlen aus dem Rechnungswesen. Diese Unterlagen sind häufig einem breiten Teil der Belegschaft zugänglich und werden für die tägliche Arbeit benötigt. Falls solche Informationen in falsche Hände geraten, entsteht ein Schaden für die Unternehmung. Institutionen im Hochrisikobereich wie beispielsweise Fluggesellschaften, Flugsicherungsbetriebe, Bahnbetriebe oder Betreiber von Kernkraftwerken lassen zum Thema «Human Factor» in Unternehmen forschen. Erkenntnisse zum menschlichen Versagen können von ihnen auch im Alltag von KMU übernommen werden:

Das Risiko eines Informations-GAUs kann eingedämmt werden. Emery hat bereits 1959 vorgeschlagen, Verhaltensbedingungen, unter denen Menschen Handlungen vollziehen – den Human Factor –, in Risikoüberlegungen miteinzubeziehen. Dazu unterscheidet er die fünf Bereiche Technik, Umwelt, Organisation, Gruppe und Individuum, die zu analysieren sind:

Human Factor Technik

Der Human Factor Technik zeigt die Gestaltung eines Systems und wie gut verständlich die Handhabung ist, zum Beispiel einer technischen Anlage, eines Computers oder sonst eines Gerätes. Nokia kam in den letzten Jahren in eine wirtschaftliche Krise. Ursprünglicher Auslöser war, dass sie ein Gerät auf den Markt brachten, bei welchem die Handhabung (Usability) nicht dem Menschen entsprach. Es konnte nicht intuitiv bedient werden, man musste sich durch Handbücher durchkämpfen, um es zu verstehen. Handhabungsfehler waren somit impliziert. Für Nokia wurde es zum Desaster, da sich das Gerät schlecht verkaufen liess. Eine technische Anlage, die konstruiert ist, dass sie gegen die gängigen Verhaltensmuster verstösst, erhöht das Risiko einer Fehlbedienung.

Die eigene Karrierearchitektur kann durch äussere Prozesse überholt werden und die tägliche Arbeit kaum mehr koordiniert ablaufen.

Leitfaden für die nächste Katastrophe Perrow (1992)	**NDB-Datendiebstahl** gemäss Presse
Das Eintreten von Unfällen wird von den Verantwortlichen als vernachlässigbar klein eingestuft.	Obwohl der fehlbare Mitarbeitende Sitzungen und Personalgesprächen fern blieb sowie Zugriffsrechte für Kollegen unterband, konnte er unbehelligt in sensiblen Bereichen weiterarbeiten. (Sonntags-Zeitung, 30.9.2012)
Nachrichten über einen eingetretenen Unfall stammen aus Quellen ausserhalb des Systems. Wobei dies in verstärktem Mass für Beinah-Unfälle gilt.	Der Hinweis, der zur Aufeckung des Datendiebstahls führte, kam von einem Kundenberater der UBS ausserhalb des NDB. (Sonntags-Zeitung, 30.9.2012 – NZZ, 30.9.2012)
Unfälle und ihre möglichen Folgen werden so weit wie möglich bagatellisiert.	Verteidigungsminister Ueli Maurer erkennt trotz des riesigen Datenklaus keine «fahrlässigen Fehler» im Nachrichtendienst. (Tages-Anzeiger, 1.10.2012)
Jeder Unfall wird – wenn irgendwie möglich – zunächst mit «menschlichem Versagen» oder «Bedienungsfehlern» erklärt.	Hoffnung macht in diesem Fall, dass auch die Ursachen im Umfeld gesucht werden.
Eingehende nachfolgende Untersuchungen müssen auf Vertuschungsversuche vorbereitet sein.	Ueli Maurer entliess die kritische zweiköpfige interne Aufsicht über den Inlandnachrichtendienst, der auf den Missstand hinwies. (Tages-Anzeiger, 2.10.2012)
Nach Abschluss der Untersuchung wird sich kaum etwas verändern.	«Die früheren Hinweise der Geschäftsprüfungsdelegation auf die Sicherheitslücken bei der Geheimdienst-Informatik hatten offensichtlich nichts genützt.» (Zitat Philipp Müller im Tages-Anzeiger, 17.10.2012)

Gefahren entstehen schleichend

Risiken im IT-Umfeld kann mit den bekannten Möglichkeiten wie Vier-Augen-Prinzip, Berechtigungskonzepten, Checklisten und Qualitätskontrollen etc. begegnet werden. Gefahren durch Unzugänglichkeiten für den Menschen entstehen jedoch häufig schleichend. So zum Beispiel wachsen eingeführte Systeme langsam über Jahre hinweg. Hier ein zusätzliches Programm, da noch eine Applikation – Insider sprechen auch von Mushrooms –, Zusatzsysteme, die wie Pilze aus dem Boden schiessen. Damit erhöht sich auch die Komplexität einer Anlage. Irgendwann kennen sich nur noch ein bis zwei Mitarbeitende sicher mit dem System aus. Sie kontrollieren ein System, das von ihnen abhängig ist, und haben ein Königreich begründet. Für Aussenstehende wird es schwierig, sich einzuarbeiten und den Überblick zu gewinnen; ein Unternehmen wird von Schlüsselpersonen abhängig und damit von ihrem Wohlwollen. Stellvertretungen werden erschwert, weil damit auch das Fehlerrisiko steigt. Beim NDB wurde zugelassen, dass der mutmasslich kriminelle Mitarbeiter alleine für einen sensiblen Systembereich zuständig ist, und Stellvertretungen wurden ausgeschaltet. Es gelang ihm, Zugriffsrechte zu blockieren, was anscheinend durch die herrschende Risikokultur zugelassen wurde.

Ein Schutz vor solchem Missbrauch kann nur gelingen, wenn sich ein Unternehmen bei der Einführung von IT-Systemen möglichst am Standard des Herstellers orientiert. Software-Hersteller, wie etwa SAP, orientieren sich bei der Entwicklung an bewährten Betriebsabläufen. Dabei werden Vorgaben aus der Betriebs-

wirtschaft, Organisationslehre, Rechtsprechung etc. berücksichtigt. Für ein Unternehmen, welches eine solche Software einsetzt bedeutet dies, es kauft sich nicht nur ein System zur effizienteren Prozessabwicklung, sondern auch eine neue Organisation. Hier steckt auch der Fehlerteufel. Über Jahre gewachsene Abläufe werden bei einer Neueinführung nicht in Frage gestellt. Die Verführung ist gross, die neue Software dem Unternehmen anzupassen. Was nicht in der Software vorgesehen ist, wird mit «Work arounds» implementiert. Die Lösung kann nur lauten: Sich an den Standards der Hersteller orientieren und möglichst nahe daran bleiben.

Human Factor Individuum

Der IT-Mitarbeitende wurde zum Spion. An der folgenden Pressekonferenz verliess der Vorgesetzte kommentarlos den Raum durch die Hintertüre, wie aus der Tagesschau am Schweizer Fernsehen zu erfahren war.

Risikoverhalten bei den Mitarbeitern kann verschiedene Ursachen haben, wie mangelnde Motivation, inadäquate Risikowahrnehmung, fehlendes Hinterfragen von Fehlern, ungesunde Identität oder ungenügende Qualifikation. Was beim NDB geschehen ist, werden vielleicht die eingeleiteten Untersuchungen zeigen. Der Presse ist zu entnehmen, dass der NDB eine Reorganisation mit Eingliederung einer andern Geschäftsstelle hinter sich hat. Dies hat Veränderungen ausgelöst.
Von den Mitarbeitenden wird bei Veränderungen hohe Flexibilität gefordert. Der Forscher Leach beschreibt zwei Arten von Veränderungen. Bei der einen wissen wir, dass sich etwas wandelt, aber es scheint eine Kontinuität mit dem Vorausgegangenen zu besitzen; bei der anderen tritt ein Bruch aufgrund von Handlungen ein, die unser Leben unwiderruflich verändern. Der Mensch kann sich zu erwartende Veränderungen kaum vorstellen, für ihn werden die Einflussfaktoren auf das Leben unkontrollierbar.

Mitarbeitenden werden bei Reorganisationen neue Arbeitsfelder zugeteilt, Vorgesetzte wechseln, der Verhaltenskodex der alten Umgebung stimmt mit den Anforderungen im Umfeld nicht mehr überein. Die eigene Karrierearchitektur wird durch äussere Prozesse überholt. Die tägliche Arbeit läuft kaum mehr koordiniert ab. Introvertierte IT-Spezialisten müssen plötzlich die Fähigkeit zur Kooperation entwickeln und mit Kollegen neue Prozesse absprechen. Eine neue Kultur ist am Entstehen.

Human Factor Gruppe

Der Datendiebstahl des NDB-Mitarbeitenden war ein egoistischer Akt, gleich was sein Antrieb dazu war. In Zeitungen war die Rede von Mobbing. Der Mensch als soziales Wesen wird durch sein Umfeld beeinflusst. Soziale Normen von unseren Kollegen, Freunden und Angehörigen prägen uns. Erwartungen werden dabei häufig nicht ausgesprochen. Durch die berufliche Sozialisation haben wir die entsprechenden Regeln eines Berufstandes verinnerlicht. Solche sozialen Normen wirken, wenn Personen den wahrgenommenen Erwartungen anderer entsprechen (wollen). Dadurch entstehen im Berufsalltag automatisch Gedanken wie «immer kompetent wirken», «keine Angst haben» oder «ich muss alles unter Kontrolle behalten». Ein Börsenhändler denkt sich vielleicht: «ich muss viel Gewinn erzielen» und geht dadurch überhöhte Risiken ein. Warum sich der IT-Mitarbeiter im NDB von der Gruppe ausgestossen gefühlt hat, kann der Presse nicht entnommen werden und ist somit reine Spekulation.

Signale wie überdurchschnittlicher Personalwechsel oder Mobbingvorwürfe deuten auf Missstände im Team und der Führung hin. Die Betriebssicherheit kann dadurch gefährdet werden, indem die Mitarbeiterloyalität gestört ist. Bei länger andauernden Missständen, kann es sich lohnen, der Sache auf den Grund zu gehen und Fachspezialisten beizuziehen.

Überdurchschnittlicher Personalwechsel oder Mobbingvorwürfe deuten auf Missstände im Team und der Führung hin.

Auswirkung ...	... für den Regel erlassenden Betrieb	... für die Regeln befolgende Person
Vorteile	• Erhöht die Vorhersehbarkeit über Personen hinweg • Definiert Aufgaben und Verantwortlichkeiten klar • Liefert eine Grundlage für die Bewertung und Durchsetzung bestimmter Handlungsweisen	• Spart Zeit und Aufwand, in bekannten Situationen «das Rad stets neu zu erfinden» • Schafft Klarheit über Aufgaben und Verantwortlichkeiten • Liefert eine Grundlage für die Einschätzung der eigenen Handlungsweise (z.B. regelkonform)
Nachteile	• Unterdrückt Innovationen der lokalen Akteure • Erschwert organisationales Lernen • Stellt hohe Anforderungen an das Management • Regelgenerierung, -verbreitung und Überwachung der Regeleinhaltung sind ressourcenaufwendig	• Erschwert das Erkennen neuartiger Situationen, die durch das existierende Regelsystem nicht abgedeckt sind. • Erlebte Einschränkung der Handlungsfreiheit kann Unzufriedenheit auslösen und die Wahrscheinlichkeit bewusster Regelverletzungen erhöhen

Quelle: Hale & Swuste (1998)

Human Factor Organisation

Fehlende Sicherheit bei den Computersystemen, eine verspätete und mangelhafte Aufarbeitung des Datendiebstahls vom Mai, unklare Strukturen bei der Beaufsichtigung der Mitarbeitenden: Die Geschäftsprüfungsdelegation (GPDel) des Parlaments richtet harsche Vorwürfe an den Nachrichtendienst des Bundes und seine Verantwortlichen, so der Tages-Anzeiger vom 17. Oktober 2012. «Ein funktionierendes Risikomanagement fehlt im NDB», kommt der Autor zum Schluss. Schweizer Firmen, so zitiert die NZZ Max Klaus am gleichen Tag, gäben mehr aus für Toilettenpapier als für Computersicherheit. Klaus ist stellvertretender Leiter der Melde- und Analysestelle Informationssicherung (Melanie) beim Bund.

Betriebe mit ihren Organisationen sind sich häufig nicht bewusst, welchen Einfluss sie mit ihren Strukturen haben. So zum Beispiel in der Aufgaben- und Arbeitsplanung:

- Unangemessene Zeitvorgaben für die Arbeitsaufgaben: IT-Systeme, die nicht fertig programmiert sind, werden eingeführt.
- Sich widersprechende Aufgaben: Von Mitarbeitenden wird verlangt, Sicherheitsregeln einzuhalten, obwohl dies durch bestehende Arbeitsvorgaben nicht möglich ist.
- Aufgaben werden nicht den Qualifikationen angepasst: Mitarbeitende werden über- oder unterfordert.
- Nicht eindeutig formulierte Aufgaben: Der Mitarbeitende versteht nicht, was eigentlich von ihm verlangt wird und wie er gemessen wird.

All diese Beispiele führen zu Unsicherheiten im Arbeitsalltag. Unsichere Handlung bedeutet einen Fehler, ein Risiko oder Frustration, was zu regelwidrigem Verhalten führen kann. Um den Arbeitskontext zu vereinfachen, streben die meisten Unternehmen eine hohe Standardisierung an. Handlungen werden vereinheitlicht, indem Mitarbeitende verpflichtet werden, Regelwerke und Checklisten einzuhalten. Diese Standardisierung bringt für Mitarbeitende Vorteile: Sie haben eine Orientierungs- und Koordinationsfunktion. Mit einer Vereinheitlichung von technologischen und organisatorischen Schnittstellen bringen sie Transparenz und eine höhere Integration verschiedener Bearbeitungsschritte. Für eine Risikoeinschätzung haben Hale und Swuste 1998 die Vor- und Nachteile von Regeln zusammengestellt (siehe Kosten S. 23).

Human Factor Umwelt

Der IT-Mitarbeitende wurde Ende Mai 2012 verhaftet. Die ersten Berichte in der Presse erschienen Ende September. Vier Monate dauerte es, bis der Vorfall durchgesickert ist. Bei Redaktionsschluss dieser Ausgabe ist der Reputationsschaden für den NDB noch nicht ausgestanden. Das Thema wird in der Öffentlichkeit weiter diskutiert. Zu einem funktionierenden Risikomanagement gehört ein Kommunikationskonzept – intern wie auch extern. Der NDB-Chef Markus Seiler will sich der Presse nicht stellen und verlässt das Bundeshaus durch die Hintertüre. Dabei benutzt und enttarnt er den geheimen Fluchtweg im Bundeshaus, welcher dem Bundesrat für den Notfall dienen sollte. Man fragt sich: «Hat der Mann keinen Kommunikationsberater?» Seiler verweigert die Kommunikation mit der Öffentlichkeit. Wobei Kommunikation nicht heisst, dass Interna ausgeplaudert werden, sondern dass Klarheit geschaffen wird über den Sachverhalt und welche Massnahmen eingeleitet werden. Im August – rund einen Monat vor der Veröffentlichung der Information zum Diebstahl – machte die GPDel das VBS auf die Wichtigkeit einer professionellen und wahrheitsgetreuen Kommunikation aufmerksam. Im September zeigte sich dann laut GPDel, dass das Departement auf eine Information der Öffentlichkeit «nur rudimentär» vorbereitet war. Aufgrund dieser Tatsache muss davon ausgegangen werden, dass die Kommunikation intern zwischen den verschiedenen Behörden ebenfalls Mängel aufweist, da sie anscheinend keine Verhaltensänderung bewirkt.

Sicherheitskultur

Der Human Factor im Risikomanagement kann berücksichtigt werden, indem eine entsprechende Sicherheitskultur bei allen Mitarbeitenden – vom Chef bis zur Aushilfskraft – gefördert und eingefordert wird. Sicherheit ist nun mal ein Prozess. ■

Merkmale hoher Zuverlässigkeit in Risikobereichen
Weick und Sutcliffe, 2003, zusammengestellt von Prof. Dr. T. Wäfler, 2008

Konzentration auf Fehler: Fehlern auf den Grund gehen
- Jeder Lapsus ist ein Hinweis darauf, dass mit dem System etwas nicht in Ordnung ist
- Fehler und Zwischenfälle werden erkannt und analysiert
- Erfolg, Selbstzufriedenheit, Routinen bergen Gefahren
- Mitarbeitende motivieren, Fehler zu melden

Abneigung gegen vereinfachende Interpretationen: Vereinfachungen kompliziert machen
- Weniger vereinfachen und mehr sehen
- Welt als komplex, unbeständig, unbegreiflich, unvorhersehbar betrachten
- Förderung von Skepsis / Gefahren von Group Think
- Meinungsunterschiede versöhnen und Gegensätze bestehen lassen

Sensibilität für betriebliche Abläufe: Betriebsabläufe als Wichtigstes betrachten
- Kontinuierliche Suche nach latenten Fehlern in den Abläufen
- Gespür für die reale Entwicklung der Situation aufbauen
- Auf latente Fehler achten, Beschäftigung (Achtsamkeit) mit Unerwartetem

Streben nach Flexibilität: das Problem behandeln (nicht verhüten)
- Fähigkeit, (unvermeidliche) Fehler rasch zu entdecken, zu begrenzen und sich davon zu erholen
- Sich von Irrtümern nicht lähmen lassen
- Gewicht auf Experten, die improvisierte Methoden einsetzen können
- Fähigkeit, Fehler frühzeitig zu erkennen und das System durch improvisierte Methoden am Laufen zu lassen

Respekt vor fachlichem Wissen und Können: Know-how vor Status und Rang
- Entscheide beim Fachwissen ansiedeln (Dezentralisierung)
- Unterschiedliche Perspektiven erhöhen Wahrnehmungsfähigkeit in komplexen Situationen und helfen, dies konstruktiv zu nutzen


RICHARD WERNER
ist Dr. MBA und seit 2003 Managing Partner der Risk Control RCC GmbH (Schweiz & Europa). Er gastiert oft als Fachreferent an internationalen Sicherheitsmessen.
GABRIELA SUTER
ist M.Sc. und Expertin für Human Factor im Risikomanagement. Sie ist Geschäftsführerin bei Suter & Co Teamwork in Eglisau.