Wenn der Blackout einen Klick entfernt ist

Beitrag

_Pierre Kilchenmann, Senior Cyber Security Expert beim Eidgenössischen Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS)
_Giorgio Tresoldi, Leiter Internationale Beziehungen und Scouting, Cyber-Defence Campus

Erschienen im SMART insights 2023 Magazin

Die Schweizer Armee bereitet sich auf Hacker-Angriffe aus anderen Staaten vor, um das Land zu schützen. Denn Cyberangriffe nehmen zu. Mit gravierenden Folgen für Gesellschaft und Wirtschaft. Bei «Locked Shields», einer der bedeutendsten Cyberabwehrübungen, hat die Schweiz bis anhin ein gutes Ergebnis erzielt. Pierre Kilchenmann hat das Schweizer «Blue Team» geleitet und erzählt von seinem Erfolgsmoment. Beteiligt war auch Giorgio Tresoldi. Seine Spezialität sind innovative Cyber-Defence-Lösungen.

Die Stromversorgung bricht ein. Der öffentliche Verkehr steht still und die medizinische Versorgung ist blockiert. Ein Schreckensszenario, das immer häufiger zur Realität wird. Hybride Kriegsführung breitet sich weiter aus. Cyberangriffe auf kritische Infrastrukturen nehmen zu. Die Bedrohung von kritischen Infrastrukturen ist vielfältig und geht über die Lahmlegung des Energienetzes hinaus. Weitere Gefahren sind etwa Datenspionage oder Datendiebstahl zwecks Erpressung. Angriffe auf die kritischen Infrastrukturen können verheerende Auswirkungen auf Bevölkerung und Wirtschaft haben. Sie gefährden die Versorgung von Gütern und Dienstleistungen, die unentbehrlich sind für eine funktionierende Gesellschaft. Gefährdet sind zudem besonders schützenswerte Personendaten – etwa biometrische Daten oder Daten aus dem Verfahrensverzeichnis.

In der Schweiz definiert der Bundesrat die kritischen Infrastrukturen. Insgesamt zählen hierzulande 10 000 einzelne Objekte als kritische Infrastrukturen. Sie sind in neun Sektoren und 27 Teilsektoren unterteilt.

Es gibt diverse Massnahmen, um kritische Infrastrukturen zu schützen – bauliche, rechtliche oder technische. Sie alle zielen darauf ab, solch schwerwiegende Ausfälle zu verhindern. Falls es doch zu einem Ausfall kommt, dienen sie dazu, die Funktionsfähigkeit schnellstmöglich wiederherzustellen. Das Szenario von «Locked Shields» erlaubt es, die Handlung bei einem solchen Ausfall durch Cyberangriffe zu üben.

Fiktiv und doch real: der simulierte Cyberangriff

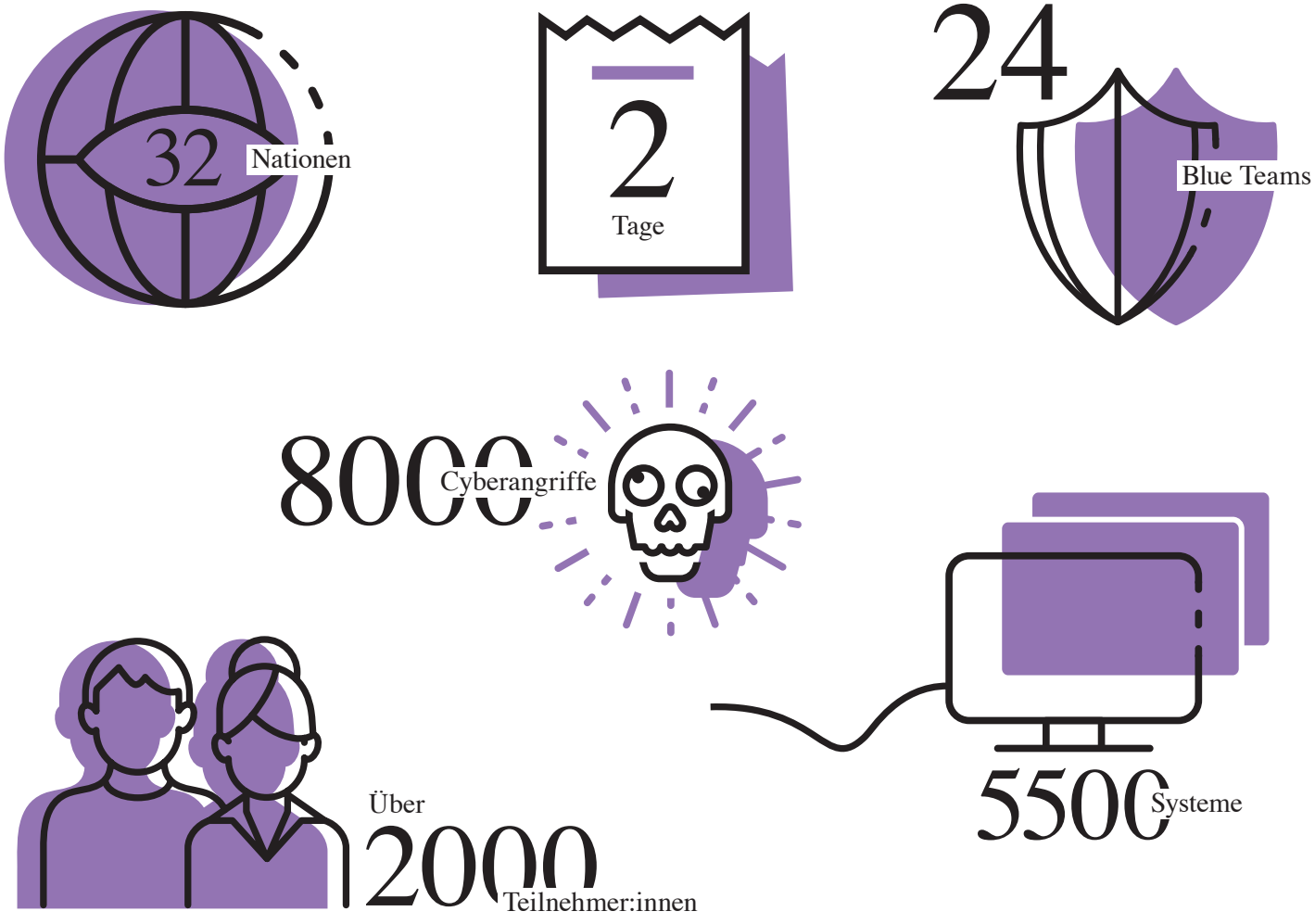
Bei der Locked-Shields-Übung wird ein gross angelegter Cyberangriff auf einen NATO-Mitgliedstaat simuliert. Während dieser Übung trainieren Fachkräfte der Schweizer Armee mit Teams aus 32 Nationen die Abwehr von Cyberangriffen. Die Simulation ist fiktiv und zugleich äusserst realitätsnah. Sie umfasst alle technologischen wie politischen Aspekte der Cyberabwehr. Es geht darum, die Kontrolle über die eigene technische Infrastruktur sicherzustellen.

Das NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn organisiert eine der grössten Cyberabwehrübungen der Welt. In Vorbereitung auf die Teilnahme an «Locked Shields» ist der Cyber-Defence Campus Partnerschaften mit innovativen Schweizer Unternehmen eingegangen. Die Fachgruppe der Armasuisse hilft, Risiken im Cyberbereich früh zu erkennen und bildet Cyberfachkräfte aus. Der Cyber-Defence Campus wählt seine Partnerschaften gezielt aus, um Werkzeuge für die Abwehr zur Verfügung zu stellen, die höchste Sicherheit bieten. Eines dieser Werkzeuge ist Airlock Gateway.

Angriff auf Schwachstellen
Die «Blue Teams», darunter das Schweizer Team, unterstützen und betreuen die kritischen Infrastrukturen eines Landes. «Red Teams» greifen im Cyberraum an, um Schwachstellen in Systemen und Prozessen zu ermitteln und auszunutzen. Die «Blue Teams» müssen die simulierten Angriffe auf den fiktiven Staat Berylia innert kürzester Zeit abwehren. Die Schweizer Armee nimmt seit 2012 regelmässig mit ihrem eigenen «Blue Team» an der Übung «Locked Shields» teil.

Schweiz erzielte gutes Ergebnis
40 Webanwendungen, zahlreiche Bugs, falsche Konfigurationen und veraltete Software sind Teil der Übung. Um die Dienste vor Angriffen zu schützen, müssen sie aktualisiert und Fehler im Programm behoben werden. Doch im Krisenfall fehlt die Zeit. Abhilfe schafft ein zentraler Airlock Gateway. Dieser erlaubt, virtuell und für alle Applikationen zusammen zu patchen – also Lücken zu schliessen. Airlock Gateway schützt unternehmenskritische, webbasierte Applikationen und APIs vor Angriffen. Künstliche Intelligenz unterstützt durch Machine Learning schützt gegen neuartige Angriffe und erkennt Bots, da sie sich anders verhalten als normale Benutzer. 2022 positionierte sich das Schweizer «Blue Team» bei der Übung unter den zehn besten Nationen. Dazu hat Airlock Gateway massgeblich beigetragen. Obwohl die Angriffe während der Übung immer raffinierter wurden, war Airlock Gateway fähig, selbst die ungewöhnlichsten Fälle zu bearbeiten. Auch bei der Durchführung 2023 von «Locked Shields» wird Airlock wieder eingesetzt.

_Cyberabwehrübung
«Locked Shields» in Zahlen

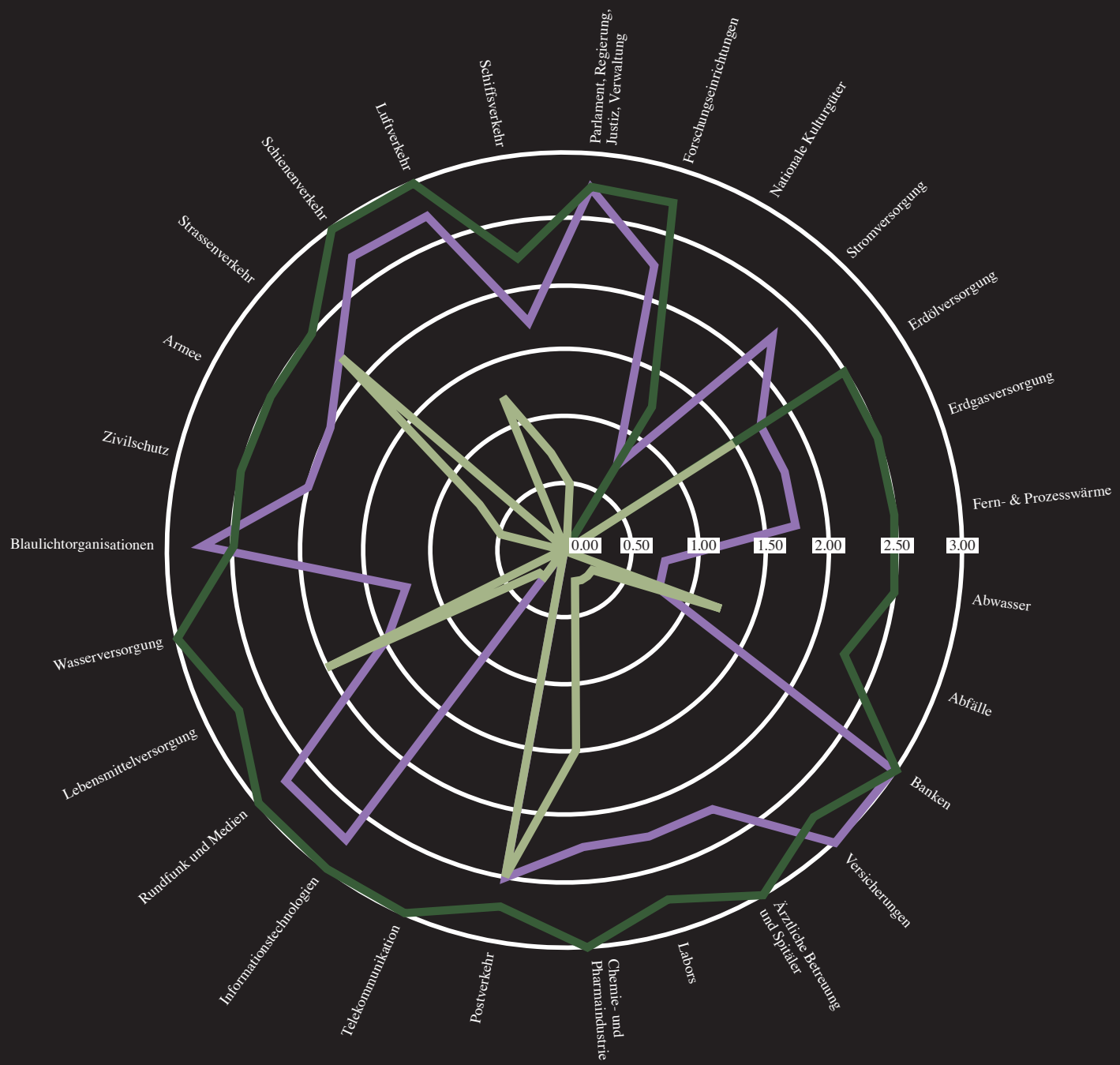


_Ein Ausfall verursacht weitere

In der Schweiz umfassen die kritischen Infrastrukturen neun Sektoren, die in 27 Teilsektoren unterteilt sind.

Fällt ein Teilsektor aus, beeinflusst dies andere Teilsektoren. So sind bei einer Störung oder beim Ausfall des Teilsektors Stromversorgung auch die Wasserversorgung, Banken oder die Chemie- und Pharmaindustrie massiv betroffen. Auf nationale Kulturgüter hat der Ausfall jedoch kaum Einfluss.

Am Beispiel von drei Teilsektoren zeigt die Grafik, wie sich die Störung oder der Ausfall eines Teilsektors auf einen anderen auswirken würde.



0.00 → 3.00

Keine Auswirkung einer Störung oder eines Ausfalls auf den Teilsektor

Sehr starke Auswirkung einer Störung oder eines Ausfalls auf den Teilsektor

- Stromversorgung
- Schienenverkehr
- Telekommunikation

Vertrauen ist die beste Verteidigung

Pierre Kilchenmann ist Teil der Führungsunterstützungsbasis (FUB) und leitet das «Blue Team» der Schweizer Armee bei der Locked-Shields-Übung. Zudem arbeitet er als Senior Cyber Security Expert beim Eidgenössischen Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS). Im Interview spricht er über die Locked-Shields-Übung und über Leadership an der Schnittstelle von starrer Armee- und agiler Cyberkultur.

Welche Bedeutung hat «Locked Shields»?
Als eine der bedeutendsten Cyber-Defence-Übungen hat sie einen unglaublichen Stellenwert. Es ist die ideale Möglichkeit, ein Extremszenario zu testen und zu erkennen, ob die Schweiz für den Ernstfall gewappnet und funktionstüchtig wäre, sprich, ob die Lagerbestände genügen würden und die menschlichen Ressourcen in Bereitschaft wären.

Und was fasziniert dich daran?
Im internationalen Kontext dem gemeinsamen Ziel entgegenzusteuern, macht diese Übung extrem wertvoll und spannend. Man lernt Profis aus zig Branchen kennen – Zivil, Militär, Industrie – und muss schnell eine Vertrauensbasis mit wildfremden Menschen schaffen. Denn Sicherheit ist ja vor allem eine Vertrauenssache.

Wie hat sich die Übung über die Jahre weiterentwickelt?
Früher war sie stärker militärisch orientiert. Mit zunehmender Digitalisierung gewann die technologische Komponente an Bedeutung, weil sie elementar ist für kritische Infrastrukturen. Darum arbeiten wir eng mit Partnern wie SBB oder Swissgrid zusammen, die ebenfalls solche Szenarien simulieren. Wir üben auch gemeinsam, damit wir einander mit Ressourcen unterstützen könnten, weil die fehlende Feinabstimmung uns im Ernstfall wertvolle Zeit kosten würde.

Die grössten Herausforderungen bei «Locked Shields»?
Bei diesem multinationalen Wettbewerb geht es natürlich ein bisschen um Nationalstolz, aber der Fokus liegt auf der Zusammenarbeit: Es gewinnt nicht, wer am besten verteidigt, sondern, wer am besten die Kooperation mit anderen fördert. Zum Beispiel, wenn ein Land Schwachpunkte findet, könnte dies Konsequenzen für Nachbarstaaten haben, also holt man sie mit ins Boot. Der Cyberraum ist hochkomplex und man kann brenzlige Lagen zwar allein überleben, aber man wird wohl kaum allein stabilisieren.

Die wichtigsten Learnings der Übung 2022?
Generell ist die effiziente Ressourcenplanung immer ein Knackpunkt, aber natürlich gab es zahlreiche Learnings auf strategischer, operativer und technischer Ebene. Da die Materie stets komplexer wird, gewinnt die Krisenkommunikation an Bedeutung. Ist die nationale Führung strategisch-politisch über die Lage präzis genug informiert, damit sie Anfragen der Presse beantworten kann? Und: Kann sie die technischen Begriffe aus dem Cyberbereich vereinfachen, sodass alle Betroffenen inkl. Bevölkerung sie versteht?

Wie fliessen die Learnings in die betreffenden interessierten Kreise?
Indem wir unsere Partner miteinbeziehen. 2023 werden Teams von Swissgrid und SBB dabei sein. Ihnen ist wichtig, nicht nur die strategisch-politische Ebene zu kennen, sondern aktiv mitzuerleben, wie es im Ernstfall läuft.

Auf der Suche nach Sicherheit

Dein schönster Erfolgsmoment?
Als ich realisierte, wie eine Vielzahl wild zusammengetrommelter Individualist:innen innerhalb von nur drei Wochen zum harmonischen Perfomance-Team zusammengewachsen ist. Sie alle haben ihr Ego zu Hause gelassen und darum viel voneinander gelernt. Das war für mich persönlich die grösste Befriedigung.

Wie schafft man das?
Man sollte nur starr militärisch führen, wo es nötig ist, ansonsten muss man sich der Cyberkultur und ihrem Mindset anpassen. Es ist wie in einer Sonderoperation: Man hat zwar jede Bewegung minutiös antizipiert und getestet, doch die Realität stellt dich immer wieder vor neue Herausforderungen. Denn in der Unendlichkeit des Cyberraums wird es wohl niemals möglich sein, jedes Detail zu planen. Darum muss man stetig in Bewegung bleiben.

Giorgio Tresoldi ist Leiter Internationale Beziehungen und Scouting beim 2019 gegründeten Cyber-Defence Campus von armasuisse Wissenschaft und Technologie. Als Kurator von Technologie und Team, und als Schnittstelle zwischen Armee, Forschung und Wissenschaft hat er den Schweizer Erfolg bei der Locked-Shields-Übung mitgestaltet. Er gibt einen Einblick in den Prozess sowie eine Einschätzung zur Lage der Schweiz als Cybernation.

Was ist dein Aufgabenbereich?
Ich durchforste den globalen Markt nach richtungsweisenden Cyber-Security-Lösungen, die den Bedürfnissen des Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport (VBS) und der Bundesverwaltung gerecht werden. Natürlich ist hier das hohe Sicherheits- und Schutzthema zentral, doch es geht im weiteren Sinne auch um Data Science und Machine Learning.

Wie hängt die Locked-Shields-Cyber-Defence-Übung damit zusammen?
Bei «Locked Shields» sind wir in vielerlei Hinsicht involviert. Wir beraten die Armee zu Technologien, die für die Übung relevant sein könnten, und wir dienen auch als Schnittstelle zu deren Beschaffung. Zudem evaluieren wir potenzielle Teilnehmer:innen. Dank unserer Forschungsprojekte haben wir ein Netzwerk an Koryphäen zu jeglichen Themen. Und da «Locked Shields» viele Daten generiert, unterstützen wir das Team bei der Auswertung. Hier kommt unsere grosse Expertise in Data Science zum Zug.

«Es steht nicht im Fokus, woher die Firma kommt, solange sie höchste Qualität liefert.» _Giorgio Tresoldi, Leiter Internationale Beziehungen und Scouting, Cyber-Defence Campus

Bei der Übung 2022 kam Airlock Gateway zum Einsatz.
Genau. Wir fanden den Einsatz von Web Application und API Protection interessant. Also sahen wir uns nach Schweizer Herstellern um, die zur Technologie auch einen Experten stellen, der noch einige Tage Militärdienst zu leisten hat, was bei Ergon der Fall war. Für uns war das die perfekte Kombination.

Wie wichtig ist der Einsatz von Schweizer Technologie?
Die Lieferkette ist auch im Bereich von Software zunehmend problematisch. Deshalb ist eine kurze Lieferkette vorteilhaft. Sie erlaubt eine bessere Nachvollziehbarkeit. Das macht Schweizer Technologie wichtig.

Beschützt uns eine Schweizer Software besser als eine andere?
Ich bin kein Fan von Pauschalaussagen. Es gibt überall auf der Welt starke und schwache Software-Firmen – das ist in der Schweiz nicht anders. Es steht nicht im Fokus, woher die Firma kommt, solange sie höchste Qualität liefert. Das neue Beschaffungsrecht legt einen grösseren Wert auf Nachhaltigkeit. Da haben Schweizer Firmen sicher ein grosses Potenzial. Selbstverständlich werden aber immer die WTO-Regeln sowie das geltende Beschaffungsrecht eingehalten.

Wie gut ist die Schweiz auf einen Cyberangriff vorbereitet?
Es ist schwierig, dies generell zu beantworten, da wir von einer grossen Bandbreite an Firmen reden – vom KMU mit drei Personen, bei dem eine Person sich um die IT kümmert, bis hin zu Milliardenunternehmen wie hiesige Pharmakonzerne – und die kann man nicht über einen Kamm scheren. Ich kann höchstens eine Aussage auf der Stufe von Bund und Armee machen: Meiner Meinung nach sind wir im Vergleich zu vielen Ländern auf einem guten Niveau. Aber es gibt natürlich immer Luft nach oben.

In welchen Bereichen siehst du Verbesserungspotenzial?
Ich denke, dass wir bei jeglichen Software-Themen, die Automatisierungen anbelangen, noch ein grosses Verbesserungspotenzial haben. Derzeit haben wir zu wenig Personen, um die Daten anzuschauen und Projekte durchzuführen. Würde man die Automatisierung erhöhen, könnte man mit gleich viel Personen mehr erreichen.

Welche Bereiche sind am ehesten einem Cyberangriff ausgesetzt?
Da gibt es unterschiedliche Ebenen und Branchen. Zum Beispiel bei «financially motivated crime» werden Organisationen angegriffen, damit sie bezahlen. In Spanien gab es Angriffe auf ein Spital und Operationen mussten verschoben werden. Die Hacker-Gangs wissen natürlich, dass ein Spital den Betrieb nicht unterbrechen kann.

Du hast erwähnt, dass die meisten Mitarbeiter:innen des Cyber-Defence Campus noch studieren.
Jährlich führen wir mit 30 bis 40 Student:innen und Praktikant:innen Projekte für das VBS durch und viele machen einen PhD, verfügen also über eine solide wissenschaftliche Basis. Was wir im Rahmen der Semester- oder Masterarbeiten anbieten, sind Anwendungsfälle, die für die Cyber Defence der Schweiz bedeutend sind. Es kann also gut sein, dass die Arbeiten von Student:innen später einmal beim VBS oder beim Bund genutzt werden, um die Cyber Defence zu verbessern. Der Cyber-Defence Campus ist aber nicht nur an der Zusammenarbeit mit der akademischen Welt interessiert, sondern auch mit der Privatwirtschaft.

Ihr bietet ja sogar einen Proof of Concept Fellowship an?
Ja, genau. Dieses Fellowship ist noch ganz neu und es geht darum, ein Produkt zu entwickeln. Bisher hat noch niemand das Fellowship absolviert, aber ich freue mich auf die zahlreichen Bewerbungen eurer Leser:innen (schmunzelt). Am besten gleich direkt an cydcampus@armasuisse.ch. />