«Unsere Politik im Bereich der Cybersicherheit muss überdacht werden»

In Anbetracht des Kriegs in der Ukraine sind die heute beginnenden Swiss Cyber Security Days aktueller denn je. Der ehemalige Cyberchef der Schweizer Armee, Gérald Vernez, erläutert die Bedeutung des Cyberspace in einem modernen Krieg und wie es um die Sicherheit im virtuellen Raum steht.

Frank Oliver Salzgeber

Swiss Cyber Security Days. Experten aus der Schweiz und aus dem Ausland präsentieren neuste Technologien rund um Cyber Security. Bild ce/a

FREIBURG Die Schweiz versteht sich als eines der technisch am höchsten entwickelten Länder der Welt. Dennoch belegt sie im Global Cybersecurity Index 2020 der Internationalen Fernmeldeunion (ITU) nur den 42. Platz von 182 bewerteten Ländern, was den Schutz vor Cybersicherheitslücken angeht.

Gérald Vernez, wieso belegt sie nur einen Mittelfeldplatz?

Die Schweiz hat gewisse Defizite, die dazu führen, dass sie trotz ihrer dichten Infrastruktur, ihrer zahlreichen Mittel und Talente nicht zu den Besten gehört. Ein Bericht des Bundesamts für Umwelt, Verkehr, Energie und Kommunikation im vergangenen Jahr zeigte die geringe Reife der Elektrizitätsinfrastrukturen im Bereich der Cybersicherheit. Die Bewertung auf einer Skala von 0 bis 4 erreichte nicht einmal die Note 1. Die Bewertung der ITU hat jedoch auch damit zu tun, dass die Schweiz den Fragebogen der ITU nicht beantwortet hat.

Wo liegen die grössten Baustellen in der Schweiz?

Wir haben immer noch das Gefühl, dass alles eine Frage der Technik ist. Aber das System muss auf der Ebene der Allgemeinbildung und des Verhaltens jedes Einzelnen gestärkt werden. Soll man den Eindruck erwecken, dass Bern uns retten wird? Oder die Armee? Nein, es ist die Arbeit von uns allen. Es gibt keine magische Lösung, die man kauft, installiert und betreibt und die es einem erlaubt, sich dann sicher an den Strand zu legen.

Haben Sie einige Zahlen, wie häufig Attacken stattfinden?

Alle Indikatoren stehen auf Rot. Die Akteure im Bereich Cybersicherheit melden Jahr für Jahr einen Anstieg. Das Problem ist, dass die Vorfälle gemessen werden müssen, und dazu müssten auch alle Opfer sie entdecken und überhaupt melden. Die Grauzone ist riesig. Der Branchenverband der deutschen Informations- und Telekommunikationsbranche schätzt, dass Deutschland aufgrund von Cyberkriminalität im Jahr 2020 eine Rechnung von über 220 Milliarden Euro hatte, was 6,6 Prozent des Bruttoinlandprodukts entspricht. Umgerechnet auf die Schweiz hätten wir einen Schaden in Höhe des Sieben- bis Achtfachen des Armeebudgets. Selbst wenn diese Zahl um einen Faktor zwei oder drei zu hoch ist, bleibt es ein Schaden, der für viele Menschen die Grenze des Erträglichen erreicht.

«Wir haben immer noch das Gefühl, dass alles eine Frage der Technik ist. Aber das System muss auf der Ebene der Allgemeinbildung und des Verhaltens jedes Einzelnen gestärkt werden.»

Gérald Vernez
Ehemaliger Cyberchef der Schweizer Armee

Was kann dagegen getan werden?

Unsere Politik im Bereich der Cybersicherheit muss überdacht werden. Die ersten Strategien waren stark auf die Technik fokussiert. Die nächste muss eine DNA der «Gesamtverteidigung» haben, bei der die gesamte Gesellschaft versteht, dass sie Teil der Lösung ist, wie im Bereich der Gesundheit. Deshalb spricht man auch zunehmend von Cyberhygiene. Es liegt an jedem Einzelnen, sich selbst zu pflegen, sich zu ernähren und körperlich zu betätigen, um die Wahrscheinlichkeit einer Krankheit zu verringern. Es wird immer einen Arzt, einen Krankenwagen und ein Krankenhaus geben müssen, aber der Hauptverantwortliche ist der Einzelne. Jede Person muss einfach in die Lage versetzt werden, seine Rolle im nationalen Cyber-Ökosystem zu spielen.

Wie hoch ist der jährliche Schaden bei Schweizer Unternehmen wegen Cyberkriminalität?

Die erste polizeiliche Statistik, die 2020 veröffentlicht wurde, sprach von etwas mehr als 24 000 digitalen Angriffen. Im Jahr 2021 waren es 30 000, was einem Anstieg von 24 Prozent entspricht. Während andere Delikte zurückgehen, steigen die Straftaten im digitalen Raum stark an.

Und noch einmal: Wir dürfen nicht vergessen, dass die Grauzone sicherlich gross ist.

Was sind Ihre Beobachtungen zum Cyberkrieg im Ukraine-Konflikt?

Im Moment sind alle erstaunt, dass es keine Cyberapokalypse gibt. Das liegt aber an diesem Krieg, von dem Russland dachte, dass es ihn schnell gewinnen könnte, vielleicht ohne grossen Cybereinsatz. Ein grosser Cyberangriff ist eine komplexe Angelegenheit, die sich nicht in zwei Tagen planen lässt. Es kann Wochen und Monate dauern, bis man unerkannt in ein System eindringen und Schaden anrichten kann.

Wenn Russland die westliche Infrastruktur angreifen würde, wäre dies eine Aggression, die für die Nato unter Artikel 5 (Wird ein Nato-Mitglied attackiert, so tritt der Bündnisfall ein, und die anderen Nato-Länder müssen militärische Hilfe leisten – Anm. d. Red.) der kollektiven Verteidigung fällt. Moskau wird es also nicht wagen. Es gibt eine ganze Palette von Erklärungen, warum die Lage im Cyberspace noch immer ruhig ist. Aber darauf würde ich langfristig nicht wetten. Der Cyberspace mit seinen sozialen Medien steht dabei an vorderster Front.

Können Kriege künftig im Cyberspace entschieden werden, oder was für einen Einfluss auf den Kriegsverlauf können Aktionen im Cyberraum haben?

Davon bin ich fest überzeugt. Aber es wird einen globalen Konflikt geben, in den die Cyberdimension eingebettet ist. Es gibt keinen «Cyberkrieg», sondern einen «Cyber im Krieg». Die Ansätze können direkt sein, mit Cyberangriffen auf IT-Systeme, oder indirekt, etwa über die Stromversorgung, von der alle Systeme abhängen, oder über die Kabelverbindungen, die die Meere durchziehen und über die mehr als 95 Prozent aller Daten übertragen werden.

Wie beurteilen und bewerten Sie die Aktionen der jeweiligen Konfliktparteien Russland und Ukraine? Wer agierte bisher erfolgreicher an der Cyberfront?

An diesem Punkt scheint es offensichtlich, dass die Ukraine den Informationskrieg gewonnen hat, der fast ausschliesslich durch den Cyberspace vermittelt wird. Wir sind in eine Logik der Hyperbeeinflussung eingetreten, deren Folgen noch nicht abzusehen sind. Was die Cyberangriffe betrifft, so beunruhigen mich diejenigen, die man nicht sieht und die langfristig vorbereitet werden und zu dauerhaften Ausfällen oder sogar zur Zerstörung führen könnten. Auf dem Papier ist vieles möglich, aber werden wir den Rubikon überschreiten? Dieser Krieg ist erst 40 Tage alt. Wir sollten uns davor hüten, bereits jetzt Schlussfolgerungen zu ziehen.

«Während andere Delikte zurückgehen, steigen die Straftaten im digitalen Raum stark an.»

Gérald Vernez
Ehemaliger Cyberchef der Schweizer Armee

Was tut die Schweiz, um sich gegen den Cyberkrieg zu wappnen.

Wie ich schon sagte, es gibt keinen Cyberkrieg – nur einen Cyber im Krieg. Panzer, Kampfflugzeuge, Artillerie und Infanterie werden für uns noch lange eine Realität bleiben. Das VBS hat 2017 eine Strategie entwickelt, die 2018 und 2021 verbessert wurde. Es wird noch nicht genug getan, aber der Weg ist richtig.

Die Schweiz will neue, hochmoderne Kampfjets anschaffen. Können diese Kampfjets durch Hackerangriffe in ihre Computersysteme zum Absturz gebracht werden?

Die einzigen berichteten und offenbar erfolgreichen Versuche wurden gegen statische Flugzeuge durchgeführt, zu denen die Angreifer praktisch Zugang hatten. Dabei handelte es sich um ältere Modelle, die zu einer Zeit entwickelt wurden, als der Cyberraum noch nicht zu den Operationssphären der Armeen gehörte. Neue Flugzeuge wie die F35 sind anders konstruiert. Ich halte es für sehr unwahrscheinlich und unverhältnismässig teuer für einen Angreifer, eine solche Möglichkeit in Betracht zu ziehen. Dieses Szenario wird vor allem durch die Fantasien derjenigen genährt, die verhindern wollen, dass die Schweiz neue Flugzeuge beschafft.

Chris Inglis

Cyberberater des US-Präsidenten in Freiburg

Chris Inglis wurde von Präsident Joe Biden zum ersten National Cyber Director ernannt. Er berät den US-Präsidenten in Sachen Cybersicherheit. Am Mittwoch wird Inglis an den Swiss Cyber Security Days im Forum Freiburg referieren.

Bevor er 2021 zum ranghöchsten Cyberverantwortlichen der USA ernannt wurde, lehrte Inglis als Professor für Cyber Studies an der US Naval Academy. Davor arbeitete der heute 68-Jährige fast 30 Jahre lang für die National Security Agency (NSA). Mehr als sieben Jahre davon war er deren stellvertretender Direktor. Die NSA ist der grösste Auslandgeheimdienst der USA mit über 40 000 Mitarbeitern und einem Etat von mehr als 10 Milliarden US-Dollar. Die NSA hat den Auftrag, die weltweite Telekommunikation zu überwachen und nach nachrichtendienstlich verwertbaren Informationen zu filtern, diese zu identifizieren, zu sichern, zu analysieren und auszuwerten. Ferner obliegen ihr das nationale Verschlüsselungswesen und der Schutz eigener nationaler Telekommunikationswege, einschliesslich der Gewährleistung der nationalen Datensicherheit und Funktion des Cyberspace.

Cyberverantwortlicher der USA: Chris Inglis. Bild zvg

Inglis ist Absolvent der US Air Force Academy und hat akademische Abschlüsse der Universitäten Columbia, Johns Hopkins und George Washington. Während seiner militärischen Laufbahn diente er 30 Jahre lang in der US Air Force und der Air National Guard. Er trat als Pilot im Rang eines Brigadegenerals in den Ruhestand. *fos*

Zur Person

Gérald Vernez

Gérald Vernez ist Gründer und Präsident der Stiftung Digivolution und Mitglied der Programmkommission Swiss Cyber Security Days 2022. Er war bis 2021 Delegierter für Cybersicherheit im VBS und damit für die Cyberabwehr der Armee verantwortlich. *fos*