«Wir müssen ein neues digitales Modell erreichen»

Sicherheit kennt im Internet keine nationalen Grenzen. Auch militärisch gewinnt das Thema immer mehr an Relevanz. Im Doppelinterview äussern sich der ukrainische Botschafter in der Schweiz, Dr. Artem Rybchenko, und Gérald Vernez, ehemaliger Delegierter des VBS für Cyberdefence, zur aktuellen Situation, zu den künftigen Herausforderungen und möglichen Lösungen.

Interview: Simon Gröflin

Herr Rybchenko und Herr Vernez, welche Bedeutung haben die Beziehungen zwischen der Ukraine und der Schweiz in Bezug auf den Erfahrungsaustausch und die Zusammenarbeit bei der Cybersicherheit?

Gérald Vernez: Früherer Delegierter Cyberdefence des VBS

Gérald Vernez: Ich spreche nicht mehr im Namen der Bundesbehörden und werde mich nicht zu den Beziehungen zwischen unseren Staaten äussern. Ich kann Ihnen nach meinen Dienstjahren sagen, dass im Bereich der Cybersicherheit Zusammenarbeit der Schlüssel zum Erfolg ist. Wer von den Erfahrungen anderer lernt, kann die Fallstricke, in die sie gefallen sind, vermeiden. Unsere Schwächen kommen immer zuerst den Aggressoren zugute.

Artem Rybchenko: Die Cybersecurity hat spätestens seit 2014 für die Ukraine an Bedeutung gewonnen, als der sogenannte Hybrid-Krieg von der russischen Seite lanciert wurde. Wir spüren wirklich den Druck, wie gegenwärtige Situationen die Angelegenheit wieder in den Fokus rücken. Jeglicher internationaler Erfahrungsaustausch ist uns daher wichtig. Und die Schweiz ist natürlich bekannt für ihre Qualität in verschiedenen Sparten.

Artem Rybchenko, ausserordentlicher und bevollmächtigter Botschafter der Ukraine in der Schweiz

Ich habe auch einige der Swiss-Cyber-Security-Days-Referate besucht und dabei viel Wissen mitgenommen. Es gibt leider nicht sehr viele Kooperationsplattformen wie die Schweiz.

Sie erwähnten die Schweizer Qualität? Welche Qualitäten wären das?

A. Rybchenko: Die Schweiz legt einen grossen Fokus auf die Cybersecurity und die Technologien basieren auf einem hohen Standard. Seit den letzten Jahren findet eine Zusammenarbeit zwischen unserem Ministerium für digitale Transformation und der Schweiz statt, für welche unser Vize-Premierminister verantwortlich zeichnet. Zudem wurden einige Memorandi zwischen unseren Staaten unterzeichnet. Wir schätzen den Inhalt und die Bedeutung dieser Zusammenarbeit wirklich sehr.

Wie gut wären unsere beiden Länder gegenwärtig für einen Cyberkrieg gerüstet?

A. Rybchenko: Leider sind wir jedes Jahr von Cyberattacken betroffen – in der Regel vor allem aus einem Land –, aber technisch gesehen, sind die Angriffe über die ganze Welt verteilt. National kritische Infrastrukturen wurden bei uns schon immer angegriffen. Zuvor richteten sich solche Attacken gegen private Institutionen, nun zielen diese Angriffe auch gegen staatliche Einrichtungen. Unsere Erfahrung ist jedoch sehr gross bei der Bekämpfung dieser Angriffsmuster.

G. Vernez: Wie gut wir für einen Cyberkrieg gerüstet wären, ist eine der komplexesten Fragen. Die Schweiz ist zurzeit vor allem mit Kriminalität und Spionage konfrontiert. Letztes Jahr wurden 24 400 Angriffe der Polizei gemeldet. Wie viele wurden jedoch nicht gemeldet? Zudem spielt der Zustand der Infrastrukturen eine Rolle, die eingesetzte Technologie, wie gut diese gewartet wird, wie gut das Personal und die Resilienz ist und wie gut wir die Bedrohung kennen und antizipieren. Es ist die Frage der Cybermaturität auf Stufe des Landes, und das ist sehr schwierig zu beantworten.

Worin bestehen die besonderen Herausforderungen zur Kriminalitätsbekämpfung und welche Rolle spielt die Kooperation der beiden Länder?

G. Vernez: Zusammenarbeit lässt sich nicht von sich aus in Gang setzen und basiert auf zwei fragilen Säulen, die ständig gepflegt werden müssen: die Identifikation gemeinsamer Interessen und Vertrauen. Gemeinsame Interessen sind nicht schwer zu definieren; man muss jedoch klare Prioritäten setzen. Die Säule «Vertrauen» ist komplizierter: Sie ist wie die Loyalität und wird mit der Zeit aufgebaut. In allen Fällen, mit denen ich zu tun hatte, hat es Jahre gebraucht: Vertrauen findet zwischen Menschen statt; es geht letzten Endes um die Chemie, die Menschen zusammenzubringen.

A. Rybchenko: Jedes Jahr gesellen sich mehrere neue Technologien dazu, die nicht nur von Staaten, sondern auch oft von Kriminellen genutzt werden. Die Möglichkeit, Kontrolle über neue Technologien zu erlangen, ist sehr anforderungsreich. Der Erfahrungsaustausch ist jedoch ein grosser Vorteil: Wir informieren unsere Partner über alle Arten von Attacken, denen wir ausgesetzt sind. Wir informieren sowohl die angrenzenden «Post-Sowjet-Staaten» als auch die Länder der EU. Die Situation der Ukraine ist speziell: Auf der einen Seite betrachten wir den europäischen Weg und auf der anderen Seite schauen wir uns – aus der Perspektive einer «Pufferzone» (ich mag diesen Begriff eigentlich nicht) – auch die Sowjet-Standards an. Primär verantwortlich für die Cybersicherheit zeichnet die Institution der Nationalen Sicherheit und Abwehr, wir haben aber auch eine Cyberpolizei gegen Verbrechen und finanzielle Kriminalität. Jedes Land ist ein wenig anders organisiert. Darum ist ein aktiver Erfahrungsaustausch so wichtig und bringt grosse Vorteile im Kampf gegen Cyberkriminalität.

> «Die Ukraine ist sehr bekannt für ihre jungen und gut ausgebildeten IT-Spezialisten.»
>
> *Artem Rybchenko*

> «Das derzeitige Wettrüsten zwischen Angreifern und Verteidigern werden die Verteidiger verlieren.»
>
> *Gérald Vernez*

Unser Chef der Armee, Thomas Süssli, plädierte an den SCSD für einen direkten Austausch mit der Hochschullandschaft, um eine Rekrutierung von mehr Experten für Data Science und Kryptografie zu gewinnen. Wie sehen Sie das?

A. Rybchenko: Der private Sektor spielt eine grosse Rolle bei den IT-Infrastrukturen. Die Ukraine ist sehr bekannt für ihre jungen und gut ausgebildeten IT-Spezialisten. Es heisst nicht umsonst «Grains and Brains». Ein Fokus unserer Bildung liegt ganz klar auf dem ICT-Sektor. Viele Hubs und Plattformen wurden in den letzten zehn Jahren sehr schnell und aktiv entwickelt. Diese Plattformen waren letztes Jahr auch Thema eines Austauschs bei einem Treffen unserer Regierung mit Frau Bundesrätin Sommaruga in Kiew.

G. Vernez: Die Ansicht des Chefs der Armee teile ich voll und ganz. Wir müssen uns jedoch von der Illusion befreien, dass wir «Cyber-Genies» am Fliessband produzieren werden. Wir machen es zwar inzwischen besser – zum Beispiel im Austausch mit der Armee, der ETH und mit dem Cyberdefence Campus von Armasuisse – und wir werden es in Zukunft noch besser machen. Aber wir können es drehen und wenden, wie wir wollen: Am Horizont 2026 werden dem schweizerischen Arbeitsmarkt laut ICT-Berufsbildung fast 20 Prozent der benötigten IT-Fachkräfte fehlen. Kompetentes Personal ist zwar wichtig, aber eben auch nicht nur, und es funktioniert nur der gesamte Ansatz.

Worin unterscheiden sich die Sicherheitskonzepte der Armee und die Cyberabwehr der beiden Länder aus der Sicht der Schweiz?

G. Vernez: Die Schweiz und ihre Armee müssen sich nicht wie einige ehemalige Sowjet-Staaten mit einer tiefgreifenden Transformation auseinandersetzen. Trotz aller Herausforderungen leben wir in einer viel linearen und ruhigeren Situation. Die Schweiz ist disruptiven Cyberangriffen auf ihre Infrastruktur ausgesetzt. Sie lebt in Frieden und zurzeit hilft ihre Armee, sie kämpft nicht. Unser föderaler Staat ist stark dezentralisiert. Kultur, Politik, Ausbildung, rechtliche Grundlagen… vieles ist unterschiedlich und demzufolge ebenfalls die Mittel und die Doktrin.

Der regionale ukrainische Stromversorger Kyivoblenergo wurde als einer der ersten Stromnetzbetreiber 2015 durch einen Cyberangriff lahmgelegt. Hat die Ukraine öfters mit solchen verheerenden Agriffen zu kämpfen?

A. Rybchenko: Kyivoblenergo ist einer unserer Hauptstromversorger. Es war eine der grössten Attacken. Wie schon erwähnt, ist unsere national kritische Infrastruktur ständig solchen Attacken ausgesetzt. Natürlich verursacht ein solcher Anschlag immer sehr viele Ängste und birgt das Risiko, sehr viele Daten zu verlieren. Eine Attacke dieses Ausmasses ist immer sehr unangenehm, aber glücklicherweise auch nicht die Norm.

Könnte sich ein solches Szenario auch in der Schweiz abspielen?

G. Vernez: Laut dem jüngsten Bericht des Nachrichtendienstes des Bundes sind zwischenstaatliche Rivalitäten so stark wie schon lange nicht mehr. Damit Staaten jedoch zu disruptiven Angriffen übergehen, muss es ein klares Spannungsfeld geben, denn staatlich geförderte Cybersabotage kommt nicht aus heiterem Himmel. Die Schweiz befindet sich glücklicherweise zurzeit nicht in dieser Situation. Das hindert einen Angreifer jedoch nicht daran, in unsere Systeme bereits heute

einzudringen, um am D-Day zuschlagen zu können. Der Cyberangriff auf SolarWinds in den USA zeigt, dass ein Angreifer, wenn er erst einmal eingedrungen ist, lange Zeit im Verborgenen bleiben kann, um dann schnell in eine Sabotagephase überzugehen. Der jüngste Angriff auf die Colonial Pipeline in den USA macht deutlich, dass bestimmte Gruppen, um Geld zu erpressen, nicht mehr davor zurückschrecken, lebenswichtige Infrastrukturen direkt anzugreifen. Selbst Gesundheitssysteme werden regelmässig ins Visier genommen. Die Schweiz ist nicht geschützter als andere Länder, unsere Neutralität ist kein Schutzschild. Im Gegenteil, sie ist ein lukratives Ziel für das Geschäftsmodell der Kriminellen.

In welchen Bereichen wollen die beiden Länder (Schweiz und Ukraine) ihre Zusammenarbeit intensivieren?

G. Vernez: Ich überlasse es den Regierungen, ihre Kooperationsstrategien zu definieren. Cybersicherheit ist ein Mannschaftsspiel, wie Fussball, es geht darum, das gesamte Spielfeld zu kontrollieren. Daher muss die gesamte Kette organisiert werden. Jedes Glied ist wichtig, vom Lieferanten bis zum Benutzer, über den Regulator und den Betreiber. Das derzeitige Wettrüsten zwischen Angreifern und Verteidigern werden die Verteidiger verlieren: Schauen Sie sich nur die Zahlen an. Es ist wahnsinnig und verlangt ein neues digitales Modell und daher strategische Innovation. Eine grosse Ambition? Ja, aber der aktuelle Weg ist eine Sackgasse, wenn man alle Parameter berücksichtigt.

> «Im Bereich der Cybersicherheit ist Zusammenarbeit der Schlüssel zum Erfolg.»
>
> *Gérald Vernez*

Was wäre denn der richtige Weg?

G. Vernez: Die primäre Frage ist, was wir wirklich brauchen, um den Wohlstand der Schweiz zu sichern, und nicht, was uns die «Hardware-Verkäufer» verkaufen wollen. Vernunft und Nüchternheit sind gefragt, und davon sind wir weit entfernt. Dann müssen wir unsere Interessen identifizieren und wissen, was um jeden Preis erreicht oder geschützt werden muss. Unsere Abhängigkeiten sind eklatant; sie werden unerträglich werden. Es ist eine Frage der Souveränität. Und um dies zu erreichen, müssen alle Faktoren – nicht nur Technologie und Hacker – berücksichtigt werden. Wir brauchen einen ganzheitlichen, systemischen Ansatz und Partnerschaften mit allen, die unsere Werte teilen. Und die Schweiz wird einige komplizierte Entscheidungen treffen müssen.

> «Die Cybersecurity hat spätestens seit 2014 für die Ukraine an Bedeutung gewonnen.»
>
> *Artem Rybchenko*

A. Rybchenko: Die Schweiz ist einer der Top-4-Investoren der Ukraine. Über diplomatische Beziehungen sprechen wir alle zwei Jahre. Es existiert auch eine Schweiz-Ukrainische Wirtschaftskommission. Dieses Jahr werden wir zudem 30 Jahre Unabhängigkeit feiern. Die Schweiz war auch eines der ersten Länder, das unsere Unabhängigkeit anerkannt hat. Auch Davos ist für uns wichtig. Letztes Jahr haben sich unsere Präsidenten dort getroffen und es war ein gutes Kick-off-Meeting für die nächsten Jahre. Ausserdem wird in Lugano dieses Jahr ein Treffen zu der wirtschaftlichen Situation nach der Pandemie stattfinden. Ich denke, wenn wir dereinst eine Art Memorandum im Bereich der Cybersecurity unterzeichnen können, wird dieses eine sehr gute Basis für künftige Kooperationen sein.

Was war die letzte Attacke, die Ihnen wirklich Sorgen einflösste?

A. Rybchenko: Jedes Jahr wird herausfordernder. Die Mehrheit der Infra-Attacken der letzten Jahre waren intensiver als in allen europäischen Ländern. Wenn eine Attacke gegen mehrere Institutionen gerichtet ist, weiss man nie, wie sich der Angriff weiterentwickelt. Während der Pandemie befanden wir uns oft im Austausch mit Fintech-Unternehmen. Alles, was online ist, kann angegriffen werden. Das Problem: Die kriminelle Seite ist oft schneller als die gute Seite.

A. Vernez: Die klassische Kriegsführung verfolgt nur ein Ziel: Zerstörung von Infrastrukturen! Wer die Infrastruktur des Gegners lahmlegt, braucht keine Truppen und keine Bomben mehr. Wenn wir keine Elektrizität mehr haben, ist das gesamte System betroffen. Was passiert, wenn Menschen auf einmal während Tagen hungern müssen und frieren? Zuerst Hamsterkäufe? Und dann? Eine Aktion hat drei Verursacher: das Wissen, wo angegriffen werden kann, die Mittel, um es durchzuführen, und der Wille, es zu tun. Sorgen machen mir die künftigen Cyberangriffe, weil von den drei genannten Faktoren ist man nur noch mit dem Willen ein wenig zurückhaltend, aber es wird bereits heute im Cyberraum ein Konflikt unterhalb der Kriegsschwelle weltweit geführt. ■