Cyber-Sicherheit bei der Satellitenkommunikation

Privatpersonen wie auch Firmen profitieren heutzutage von einer schnellen Satellitenkommunikation. Dabei nehmen sie in Kauf, dass ihre Daten unverschlüsselt versendet werden und somit abhörbar sind. Forschende des Cyber-Defence Campus armasuisse haben eine Lösung gefunden, wie Datentransfer über Satelliten schnell aber dennoch geschützt verlaufen kann.

Text: Dr. Vincent Lenders

Satellitenkommunikation gewinnt im zivilen und militärischen Bereich zunehmend an Bedeutung.

Kaum jemand verwendet heute noch ein WLAN ohne Verschlüsselung, denn ohne Schutz könnte der Nachbar oder eine unbekannte Drittperson den Datenverkehr abhören. Doch was für das WLAN schon seit langem üblich ist, scheint für die Satellitenkommunikation noch wenig beachtet zu sein, wie Dr. Vincent Lenders, Leiter des Cyber-Defence Campus bei armasuisse feststellt. Noch immer senden grosse internationale Konzerne und selbst Betreiber kritischer Infrastrukturen ihre schützenswerten Daten über Satellitenkommunikation völlig unverschlüsselt. Im Extremfall kann hier nicht nur der Nachbar mithören, sondern Millionen von neugierigen Personen, denn Satellitensignale können problemlos über grosse Flächen empfangen und mit einfachen Mitteln abgehört werden. Wie kann das sein?

CYBER-DEFENCE CAMPUS (CYD)

Der CYD Campus wurde im Januar 2019 unter der Federführung von armasuisse Wissenschaft und Technologie gegründet. Er ist ein Element des «Aktionsplan Cyber-Defence VBS» und zielt darauf ab, den Schutz vor Cyber-Angriffen zu optimieren sowie den Herausforderungen im Cyber-Raum künftig angemessen zu begegnen. Hierfür versorgt er das VBS mit Informationen zu rasanten Entwicklungen, angewandter Forschung, Ausbildung und Technologie-Monitoring im Bereich der Cyber-Abwehr.
Das primäre Ziel des CYD Campus ist die Antizipation von Cyber-Entwicklungen. Als Cyber-Kompetenzzentrum agiert er als Plattform zur Identifizierung und Bewertung von Technologien, kommerziellen und sozialen Cybertrends sowie den daraus resultierenden Nutzungsszenarien. Dadurch ist er ein Bindeglied zwischen VBS, der Industrie und der Wissenschaft in allen cyber-relevanten Themen.

Schneller Datentransfer, aber fehlender Datenschutz

Eine Satellitenkommunikation ist sehr praktisch und für Anwenderinnen und Anwender äusserst bequem. Das liegt daran, dass diese Art der Kommunikation von jedem Ort auf der Erde funktioniert, solange kein Hindernis zwischen einer Antenne auf der Erde und dem dazugehörigen Satelliten im Weltall besteht. So setzen auch grosse Schweizer Konzerne und Betreiber kritischer Infrastrukturen diese Technologie ein, um sich mit ihren Aussenstellen auszutauschen oder Verbindungen mit Schiffen und Flugzeugen sicherzustellen. Neben diesen Vorteilen hat die Kommunikation via Satellit aber auch einen wesentlichen Nachteil: Die sehr grossen Distanzen zu den Satelliten, welche ca. 36 000 km betragen, führen zu spürbaren Zeitverzögerungen in der Datenübertragung. Das ist für Anwendungen wie zum Beispiel Fernsehen oder auch Geolokalisierung kein Problem. Aber beim Surfen im Web führen diese Verzögerungen zu sehr langen Ladezeiten der Webseiten. Darum setzen heutige Satellitenbetreiber gerne sogenannte Beschleunigungs-Proxies ein, um die Surfgeschwindigkeit zu steigern. Solche Proxies arbeiten als Vermittler zwischen Sender und Empfänger und können durch gezielte Anpassung des Kommunikationsprotokolls die langen Verzögerungen kompensieren.

Aber genau da liegt die Krux. Wenn Firmen ihre Daten zum Beispiel mit einem VPN, also einem privaten virtuellen

Die sehr grossen Distanzen zu den Satelliten führen zu spürbaren Zeitverzögerungen in der Datenübertragung.

«Viele Firmen sind sich der Problematik nicht bewusst, weil sie denken, dass der Satellitenbetreiber eine Verschlüsselung einsetzt.»

Netzwerk, verschlüsseln, schaffen es diese Proxies nicht, den Datenverkehr zu beschleunigen, weil sie den Schlüssel dazu nicht haben. Deswegen besteht die Gefahr, dass viele Anwender und Anwenderinnen sowie auch grosse Firmen auf gängige Verschlüsselungsmethoden verzichten, in der Hoffnung, dass keine Unbefugten den Verkehr abhören.

Fehlendes Bewusstsein für die Folgen einer fehlenden Datenverschlüsselung

Genau zu dieser Erkenntnis kommen die Forschenden des Cyber-Defence Campus von armasuisse. Sie zeigen auf, dass der Datenverkehr vieler Firmen, hierzu zählen auch sensible Daten, nicht verschlüsselt ist. Mehr noch, sie können mit einem Software Defined Radio, welches drahtlose Signale von Kommunikationssystemen mittels Software verarbeiten kann, problemlos abgehört werden. Es ist also anzunehmen, sagt Dr. Martin Strohmeier, ein Experte des Cyber-Defence Campus, dass Firmen heute systematisch über Satellitenkommunikation ausspioniert werden. Und er fügt hinzu: «Viele Firmen sind sich der Problematik nicht bewusst, weil sie denken, dass der Satellitenbetreiber eine Verschlüsselung einsetzt.» Dem ist aber in den meisten Fällen nicht so.

Erarbeitung neuer und sicherer Verschlüsselungsmethoden dank Kooperationen

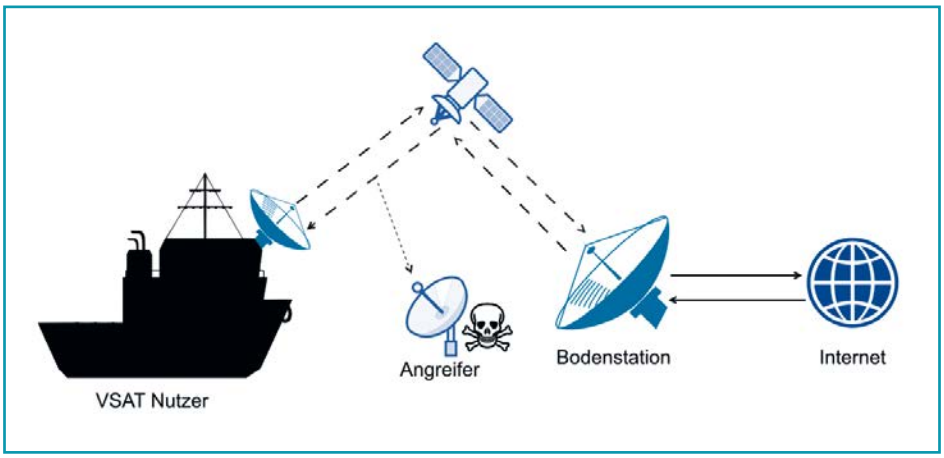
Heutzutage müssen sich Firmen also noch entscheiden zwischen Geschwindigkeit und Sicherheit. Dies könnte sich in der Zukunft aber ändern. Denn Mitarbeitende des Cyber-Defence Campus forschen seit 2019 zusammen mit nationalen und internationalen Hochschulen an neuen Lösungen. Bereits im Frühling dieses Jahres konnten die Forschenden einen ersten Prototyp eines neuen Proxies in Thun vorstellen, der in der Lage ist, den Datenverkehr zu verschlüsseln ohne dass dabei an Geschwindigkeit eingebüsst werden muss. Anwenderinnen und Anwender von Satellitenkommunikation sollen also in Zukunft, wie heute schon bei der Kommunikation über WLAN der Fall, schnelle und sichere Kommunikation geniessen können. Insbesondere Privatpersonen sowie Betriebe mit sensiblen und schützenswerten Daten, zu denen auch die Armee gehört, könnten davon stark profitieren. Bis zur weltweiten Anwendung bedarf es aber noch Anpassungen und Abklärungen. Ein erster Einsatz dieses neuen Proxies ist für das Jahr 2021 bei armasuisse in Thun geplant.

DR. VINCENT LENDERS
Leiter Fachbereich und Direktor CYD Campus

Dr. Vincent Lenders arbeitet seit 2008 bei armasuisse Wissenschaft und Technologie. Als Leiter des Fachbereichs Cyber Sicherheit und Data Science und Direktor des Cyber-Defence Campus stehen die Beobachtung der technologischen Entwicklungen und Bedrohungen im Cyberraum auf dem täglichen Programm. Hierbei werden Einsatzsysteme auf deren Sicherheit geprüft und laufend neue Technologien erforscht, um die grösstmögliche Cyber Sicherheit zu gewährleisten.

FORSCHUNGSPROGRAMM CYBERSPACE UND INFORMATION

Das Forschungsprogramm «Cyberspace und Information» stellt den Aufbau von Fachkompetenzen im Bereich der Cyber- und Informationstechnologien sicher. Hierzu gehören auch die Analyse von Informationen aus dem Cyberspace wie auch die Beurteilung der damit zusammenhängenden Risiken, insbesondere im militärischen Umfeld. Die Forschungsfelder erstrecken sich von der Cyber Sicherheit, zu Informationsmanagement bis hin zu Machine Learning und Data Science.



Eine Form der Satellitenkommunikation ist die Schiff-Land-Kommunikationstechnologie, auch VSAT genannt, welche in dieser Grafik abgebildet ist. Ein Angreifer kann problemlos die VSAT Kommunikation abhören, wenn diese nicht mit einer Verschlüsselung geschützt ist.

Forschungsdemonstrator in Thun: Eine auf dem Dach montierte Satellitenschüssel, welche Daten verschlüsselt sendet und empfängt ohne an Geschwindigkeit einzubüssen.