SCiON : Sicherheit made in Switzerland

Autor(en): **Besse, Frederik**

Objekttyp: **Article**

Zeitschrift: **Schweizer Soldat : die führende Militärzeitschrift der Schweiz**

Band (Jahr): **97 (2022)**

Heft 11

PDF erstellt am: **12.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-1045866

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

SCiON: Sicherheit made in Switzerland

Mittels einem neuen Protokoll soll das Internet sicherer werden. Die Lösung liegt auf der Hand: Lieber ein neues Netzwerk erstellen, als ein veraltetes System renovieren. Die Anbieter versprechen dabei das «sicherste Internet der Welt».

Hptm Frederik Besse

Heutzutage sind Cyberangriffe nicht nur tagtäglich zu erwarten, sondern auch erst noch günstig durchzuführen. Militärisch gesehen ist es nahezu unmöglich, die Stellung lückenlos zu verteidigen.

Was aber, wenn man sich auf vorteilhaftes Gelände bewegen würde? Metaphorisch gesehen handelt es sich beim SCiON-Internet genau um diese Idee.

Anstatt dass man im Internet von allen Ecken angreifbar ist, baut man sich quasi ein privates Netzwerk auf – mit der flexibilität des Internets.

Made in Switzerland

Am Herbsttreffen der Parlamentarischen Gruppe Cyber wurden in verschiedenen Vorträgen die Vorteile des SCiON-Internets erläutert. Der Titel der Veranstaltung lautete: «Das sicherste Internet der Welt ist online – Swiss Made Technologie, Einsatz & Potential.»

Wackliges Fundament

Bevor man verstehen kann, wie das SCiON-Internet funktioniert, muss man zuerst den aktuellen Standard kennen. Martin Bosshardt, CEO von ANAPAYA, beschrieb das so: «Das alte Internet ist eigentlich ein Wunder, denn es verbindet etwa 90 000 verschiedene Netzwerke.»

Das Internet ist somit nicht ein grosses Netzwerk, sondern ein Verbund aus Netzwerken. Das bisherige Protokoll, quasi die Passierscheine, wie man diese Netzwerke erreicht, wurde in den 90er-Jahren pragmatisch auf einem Taschentuch erstmals skizziert. Die Rede ist dabei vom Border-Gateway-Protokoll.

Dieses Protokoll ist sehr mächtig, was die Verbindungsmöglichkeiten angeht, aber hat grosse Schwierigkeiten, wenn es um die Sicherheit der übermittelten Daten geht.

SCiON soll dieses Border-Gateway-Protokoll ablösen. Damit verspricht man sich, das sicherste Internet der Welt anzubieten. Der Grund ist einfach: Im alten Protokoll kann man die ganze Welt von einem Ort aus angreifen. In einem SCiON-Netzwerk sind die Pfade, über die Daten übertragen werden, Angreifern nicht mehr bekannt. Man tarnt das eigene Netzwerk vor dem Zugriff durch Unberechtigte.

Kritische Infrastruktur

SCiON kann auch für die Regierung interessant sein. Insbesondere, wenn es um den Schutz von kritischer Infrastruktur geht.

Gruppe Cyber

Die Parlamentarische Gruppe Cyber ist eine überparteiliche Gruppierung und dient der Vernetzung von Politik, Industrie und Wirtschaft rund um das Thema Cybersicherheit. Das Co-Präsidium wird durch die Nationalräte Doris Fiala (FDP), Edith Graf-Litscher (SP), François Pointet (GLP), Gerhard Andrey (Grüne), Ida Glanzmann-Hunkeler (Mitte) sowie Bruno Walliser (SVP) sichergestellt.

Als funktionierendes Ökosystem im Internet funktioniert es bereits heute. Dabei wird trotz des zusätzlichen Schutzes auch die Verfügbarkeit des Netzes nicht beeinträchtigt. Man kann es sich so vorstellen, dass man heute auch miteinander telefonieren kann, wenn man unterschiedliche Telefonanbieter hat. Man muss aber die Nummer des Gegenübers kennen. So etwa soll auch die Kompatibilität mit dem SCiON-Internet mit dem bisherigen Internet funktionieren.

Öffentlicher Quellcode

Grundsätzlich könne jedermann selbst den Quellcode des SCiON-Protokolls ansehen und es selbst implementieren. Da dies aber Aufwand und Expertenwissen für die Implementierung erfordert, gibt es auch die Möglichkeit, dies via einem Service Provider wie ANAPAYA abzuwickeln.

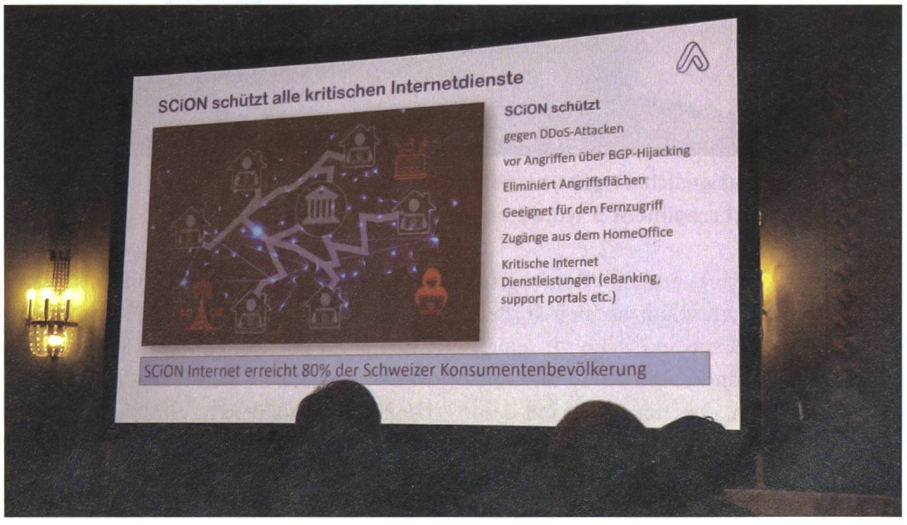

Bild: SCHWEIZER SOLDAT

Anlässlich des Herbstreffens der Parlamentarischen Gruppe Cyber wurde SCiON vorgestellt. Es soll sich sowohl für Betreiber kritischer Infrastrukturen wie auch Firmen, die ihre Angestellten im Homeoffice beschäftigen wollen, eignen.

Mobile Vernetzung in der Armee

Eine gestärkte Logistik, vorausschauende Wartung und bessere Entscheidungsgrundlagen gerade in Krisensituationen: Vernetzte Systeme bergen für die Armee enormes Potenzial – sofern die Datensicherheit jederzeit gewährleistet ist.

Transportfahrzeuge, die in Echtzeit Daten zu Treibstoff oder Betriebsstunden übertragen; Drohnen, die Aufklärungsbilder live an eine zentrale Plattform übermitteln; Panzer, die bei kritischem Betriebszustand Alarm schlagen, oder gar Sensoren, die eine permanente Überwachung der Vitalzeichen von Soldaten erlauben – modernes Equipment birgt einen enormen Datenschatz. Gerade im Militär hat die mobile Vernetzung von Personen, Fahrzeugen und weiteren Systemen ein riesiges Potenzial.

Vorteile vernetzter Systeme

- *Vorausschauende Wartung:* Über die Analyse von Betriebsstunden und Daten (Flottenzustand, Vibration, Temperatur, Verschleiss etc.) kann die Wartung besser geplant werden. Das verbessert den effizienten Betrieb von Equipment und beugt ungeplanten Stillständen vor.
- *Kürzere Reparaturzyklen:* Zeitnahe Informationen über defekte Systemkomponenten im Feld erlauben die frühzeitige Organisation von Ersatzteilen und Personal für die Reparatur.
- *Optimierte Logistik:* Die kontinuierliche Transparenz über beispielsweise Munitions- und Treibstoffvorrat verbessert die Planungsgrundlage und optimiert die Versorgung.
- *Verbesserte Entscheidungsgrundlagen:* Das gezielte Erfassen und Analysieren von Felddaten erleichtert die Entscheidungsfindung.
- *Überblick in Krisen:* Der direkte Zugriff auf operationsrelevante Daten hilft, bei Katastrophen und in Krisensituationen schneller zu handeln.

Sicherheit der vernetzten Systeme ist zentral

Die Chancen liegen auf der Hand. Doch das enorme Volumen der Daten (zum Beispiel von hochaufgelösten Bildern oder Videos), die notwendigen Übertragungsleistungen und sichere Vernetzungsmöglichkeiten stellen das Militär vor grosse Herausforderungen. Gerade im militärischen Bereich können kompromittierte oder manipulierte Informationen katastrophale Folgen haben. Informationen über Standort, Anzahl und Zustand der Truppen müssen stets geschützt sein.

Die Gefahr von Zugriffen Unberechtigter wird umso grösser, je mehr netzwerkfähige Elemente wie Sensoren, Fahrzeuge, Speicher, Software und Endgeräte zu einem Ökosystem verschmelzen. Die Sicherheit aller Elemente und Schnittstellen muss darum oberste Priorität haben. Besonders wichtig sind unter anderem das Management der Endpunkte, die sichere Kommunikation auch über «unsichere» Kanäle wie öffentliche und hybride Netzwerke, höchster kryptografischer Schutz sowie die Update- und Überwachungsfähigkeit der Systeme.

Fundiertes Expertenwissen für höchste Ansprüche

Herstellern und Anwendern fehlen aber oft die Ressourcen oder das nötige Fachwissen, um diese hohen Sicherheitsansprüche zu erfüllen. Die CyOne Security bringt fundiertes Expertenwissen in die Sicherheitskonzepte des Militärs. Eine für die mobile Vernetzung ideale IP/VPN-Technologie, gehärtete Hard- und Software sowie höchste Performance in der Datenübertragung sind nur einige der Leistungen, die sie erbringt – für höchste Sicherheit der einzelnen Komponenten sowie des Systems als Ganzes.

Erfahren Sie mehr über die Sicherheitskonzepte und -lösungen für Schweizer Behörden.

Reto Amstad, Senior Security Consultant, Tel. +41 41 748 85 16
reto.amstad@cyone.ch, www.cyone.ch

Sichere Schweiz. Bit für Bit.

Cyber-resiliente Vernetzung

CyOne Security bietet 360°-Sicherheitskonzepte und -lösungen für maximale Cyber-Resilienz.

Cyber Security aus der Schweiz. Für die Schweiz.

cyone.ch

CyOne SECURITY