

Ist SCION unangreifbar und unaufklärbar?

Studiengang : MAS Cyber Security

SCION schützt die Integrität von Kommunikationswegen im Internet. Aber es sind Weiterentwicklungen notwendig, um die Vielzahl unterschiedlicher Anwendungsbedürfnisse abzudecken.

SCION (Scalability, Control and Isolation on Next-Generation Networks), eine von der ETH Zürich entwickelte Internetarchitektur, schützt die Integrität von Kommunikationswegen im Internet.

Das Ziel von SCION ist es, die Kommunikationswege im Internet sicherer zu machen und Angriffe wie DDoS und BGP-Hijacking zu verhindern. Mit kryptografischen Massnahmen schützt SCION die Integrität der Kommunikationspfade und kann damit die Verfügbarkeit der IT-Dienste in einer Domäne erhöhen.

Die erste praktische Anwendung dieser Architektur ist das Swiss Secure Finance Network (SSFN), welches dem Schweizer Finanzplatz eine sichere Kommunikationsplattform bietet.

Problematic der heutigen Internetarchitektur

Die Zahl der Cyberangriffe auf Unternehmen, kritische Infrastrukturen und Einzelpersonen wächst mit der zunehmenden Vernetzung in der digitalen Welt überproportional an. Dabei spielen monetäre, politische und ideologische Interessen von Hackergruppierungen eine Rolle. Die Hauptziele von Hackerangriffen sind Datendiebstahl, Datenmissbrauch, Datenmanipulation, Kontrolle über die IT-Infrastruktur und Informationsfluss.

Während sich ein Teil der Angriffe auf den Inhalt der Daten konzentriert, gibt es auch Angriffe auf die Kommunikationswege im Internet. Dazu gehören DDoS-Attacken, welche mit gezielten und grossen Mengen von Anfragen ein IT-System lahmlegen können. Ziele

können IT-Systeme von Unternehmen, NGO oder staatliche Organisationen sein.

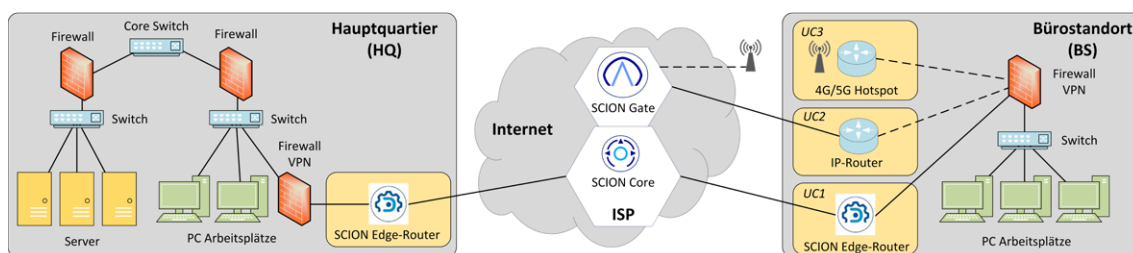
Auch Meldungen wie 'BGP-Hijacking' sind oft in den Medien zu lesen. Mit solchen Angriffen wird versucht, Kommunikationspfade im Internet zu übernehmen und an Informationen aus den Datenströmen zu gelangen. Oft stecken wirtschaftlich oder politisch motivierte Akteure hinter solchen Angriffen. Mit SCION lässt sich die Zahl solcher Angriffe minimieren.

In Bereichen vom VBS gibt es Bestrebungen, SCION als Basis für eine sichere Kommunikation über öffentliche Netze als Ergänzung zur eigenen Netzwerkinfrastruktur zu nutzen. Dabei sollen kleine Bürostandorte und temporäre Arbeitsplätze über SCION erschlossen werden.

Die Arbeit befasst sich mit Möglichkeiten und Risiken mit SCION und dem Aufbau einer Architektur, über welche sensible Daten über ein öffentliches Netz versendet werden können. Dafür wurden drei Anwendungsfälle untersucht (s. Abb.). Für Anwendungsfall UC1 wird SCION als Alternative zu eigenen Glasfaser- oder Kupferleitungen erachtet. Die Verbindungen zwischen SCION Edge-Router und SCION Core sind durch kryptografische Massnahmen integritätsgeschützt. Die anderen Anwendungsfälle, welche eine Verbindung zum SCION Netzwerk mit einem konventionellen IP-Router oder einem 4G/5G Hotspot zu einem SCION Gate herstellen, sind für die betrachteten Einsatzzwecke nicht zu empfehlen. Mit der Entwicklung eines portablen SCION Edge-Routers könnten die Risiken für diese beiden Anwendungsfälle verringert werden.



Patrick Hager
MAS Cyber Security
patrick.hager@gmx.ch



SCION Laboraufbau