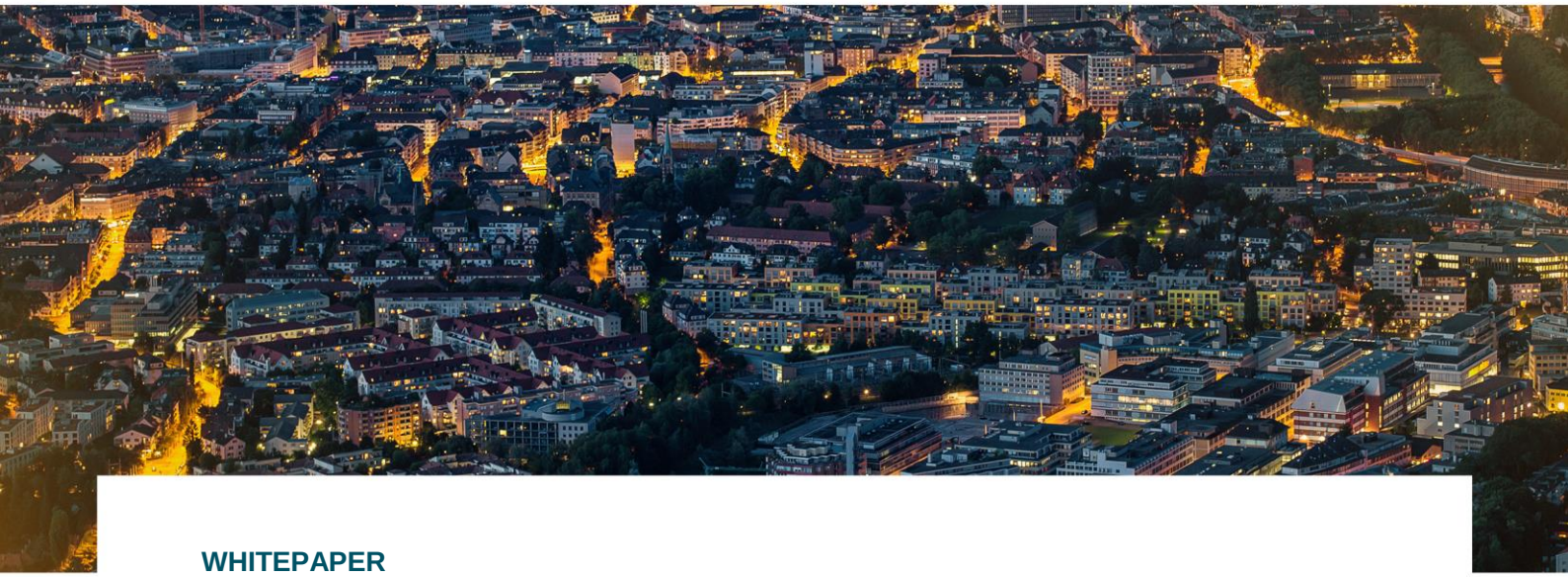
CyOne Security AG
Hinterbergstrasse 18
6312 Steinhausen

Telefon +41 41 748 85 00
info@cyone.ch
cyone.ch



WHITEPAPER

Multi Identity Network Access (MINA) – damit sich Cyber-Ermittler im Internet getarnt bewegen können

Reto Amstad | Senior Security Consultant | Steinhausen, 29. September 2020

Eine grosse Herausforderung für Cyber-Ermittler ist es, sich unauffällig und konsistent im Internet und innerhalb des Darknets bewegen zu können: Von ihrem in einem Verwaltungs-umfeld (Bund oder Kanton) eingebetteten Ermittlerarbeitsplatz bzw. von ihrem Arbeitsumfeld aus, sollen die Ermittler Täter im Netz identifizieren und cyberkriminelle Tätigkeiten bekämpfen. Dieses Whitepaper zeigt auf, wie sich Cyber-Ermittler mit verschiedenen Tarnidentitäten konsistent im Internet bewegen können.

Eines ist klar: Professionelle Cyber-Kriminelle agieren im Internet und im Darknet immer vorsichtiger und unterziehen ihre jeweiligen Kommunikationspartner oder Besucher immer öfter einer gründlichen Überprüfung. So werden IP-Adressen, User-Agents, Cookies, verwen-dete Kreditkarten, Social-Media-Einträge etc. sorgfältig geprüft. Eine kleine Inkonsistenz – und Misstrauen ist geweckt.

Um diese Ermittlungsarbeiten trotzdem erfolgreich durchführen zu können, müssen für die Strafverfolgungs- und Sicherheitsbehörden entsprechende professionelle Werkzeuge (neben TOR, I2P und anderen Anonymisierungstools) zur Verfügung gestellt werden, die keine verräterischen inkonsistenten Spuren im Netz hinterlassen.

Mit MINA (**M**ulti **I**dentity **N**etwork **A**ccess) will die CyOne Security einen Lösungsansatz aufzeigen, um die Cyber-Ermittlung in ihren Herausforderungen künftig unterstützen zu können.

Für eine effektive Cyber-Ermittlung ist es unter anderem wichtig, sich unauffällig und konsistent im Internet und innerhalb des Darknets bewegen zu können. Problematisch wird es, wenn die Ermittler ihre Tätigkeit von ihrem Arbeitsplatz aus ohne entsprechende Werkzeuge ausüben müssen. Die zur Verfügung gestellte Infrastruktur ist meistens in einem Verwaltungsumfeld (Bund / Kanton) eingebettet. Zudem können für die Ermittlungsarbeit nicht immer öffentliche Anonymisierungsnetze wie TOR oder I2P verwendet werden. Oft sollen ganz normale Internetbenutzer-Profile zur Anwendung kommen.

Erschwerend sind in diesem Zusammenhang auch die vielen fallbezogenen und oft wechselnden Tarnprofile, welche für die Arbeit der Behörden im Internet zwingend benötigt werden. So verlangen die verschiedenen Profile ja auch andere internetfähige Geräte (Notebooks, Tablets und Smartphones) und wechselnde Internetzugänge (u.a. auch geografisch getrennt). Jeweils eine dezidierte Hardware kaufen zu müssen, um in einem Starbucks-Café mit öffentlich zugänglichem Wireless-Zugang einigermassen anonym ins Internet zu gehen, kann nicht die Lösung sein.

Wird diesen Sicherheitsanforderungen aber nicht genügend Beachtung geschenkt, erhöht sich die Gefahr für das Auffliegen einer laufenden Ermittlung oder das Auffliegen der entsprechenden IT-Ermittler-Infrastruktur – dies infolge eines inkonsistenten Netz-Profils.

MINA-Funktionsumfang
Mit MINA will die CyOne Security einen Lösungsansatz aufzeigen, der die verschiedenen Sicherheitsbehörden von Kanton und Bund und die dort tätigen Cyber-Ermittler künftig in der Bekämpfung von Cyber-Kriminalität unterstützen kann – und zwar von ihren jeweiligen Arbeitsplätzen aus.

Dabei soll MINA für die Cyber-Ermittler die nachfolgenden Funktionen bereitstellen:

- Der Ermittler kann sich vorgängig aus verschiedenen Benutzerprofilen, Betriebssystemen und Hardwareprofilen passende Tarnidentitäten zusammenstellen
- Fallbezogen und konsistent kann er die definierten Tarnidentitäten einfach anwenden. Konsistent heisst in diesem Fall:
    - Anwendung der vordefinierten Hardware-Parameter gegenüber dem Internet-Service Provider und Telekom-Service Provider, gegenüber den Servern, Social-Network-Communitys und den Zielgruppen (z.B. verschiedene Betriebssysteme, User-Agent, MAC-Adressen, IMEI etc.)
    - Anzeigen der notwendigen Tarnidentität-Metadaten (z.B. Personalien, E-Mail, Social-Media Accounts etc.) während der Ermittlung, um Fehlerquoten zu verkleinern
- Sichere, lückenlose und fallbezogene Speicherung der durchgeführten Ermittlungstätigkeiten
- Verschiedene Betriebssysteme emulieren (Windows, Macintosh, Android, iOS)
- Unterschiedliche, konfigurierbare und geografisch getrennte eigene Proxy-Zugänge benutzen, und zwar über unterschiedliche Access-Medien (DSL, GSM 4G-Data, Public-Wifi)
- Durch eine einzigartige Sicherheitsarchitektur eine hochisolierte und dadurch geschützte Ermittlerinfrastruktur zur Verfügung stellen können
- Optional: Über ein zentrales SIM-Management zu verfügen unter Einbezug einer Virtual-SIM Architektur (inkl. SIM-Emulatoren). Dadurch können SIM-Karten an einem zentralen Punkt schnell gewechselt resp. an eine andere Geo-Lokalität migriert werden
- IMEI-Wechsel durchführen, um mittels SIM-Kartenwechsel ein anderes mobiles Profil zu erstellen

- Mandantenfähig sein, damit eine MINA-Infrastruktur durch mehrere Sicherheitsbehörden (z. B. innerhalb der kantonalen Polizeikorps) verwendet werden kann. Die entsprechende Datenhoheit sowohl über das verwendete Profil wie auch über die anfallenden Ermittlerdaten bleiben dank einer hohen Isolierung bei der entsprechenden ermittelnden Behörde bestehen
- Schnittstelle für einen sicheren Datenimport und -export in ein klassifiziertes Behördennetz (kompatibel mit der Coyne Security-Datenschleuse)
- Sicherer Remote-Zugriff auf die MINA-Infrastruktur für mobile Cyber-Ermittler (Roadrunner-Ansatz) wird ermöglicht

MINA-Architektur

Nachfolgende Abbildungen zeigen schematisch die Architektur des zukünftigen MINA-Systems. Dies einerseits als Einzelbetreiber-Modus (siehe Abbildung 1) und andererseits im Mandanten-Modus (siehe Abbildung 2).

Abbildung 1: Schematische MINA-Architektur

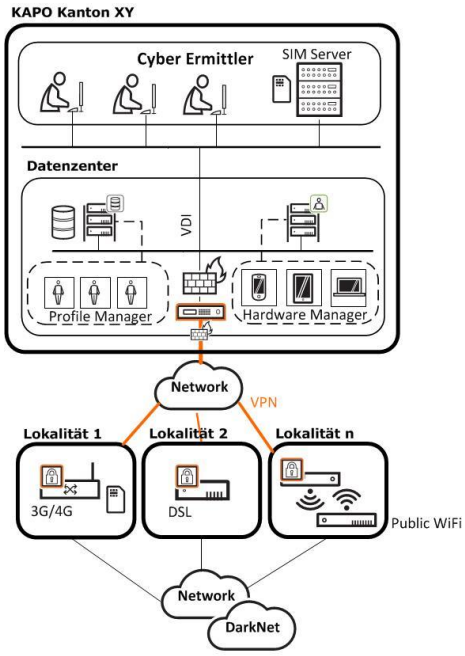
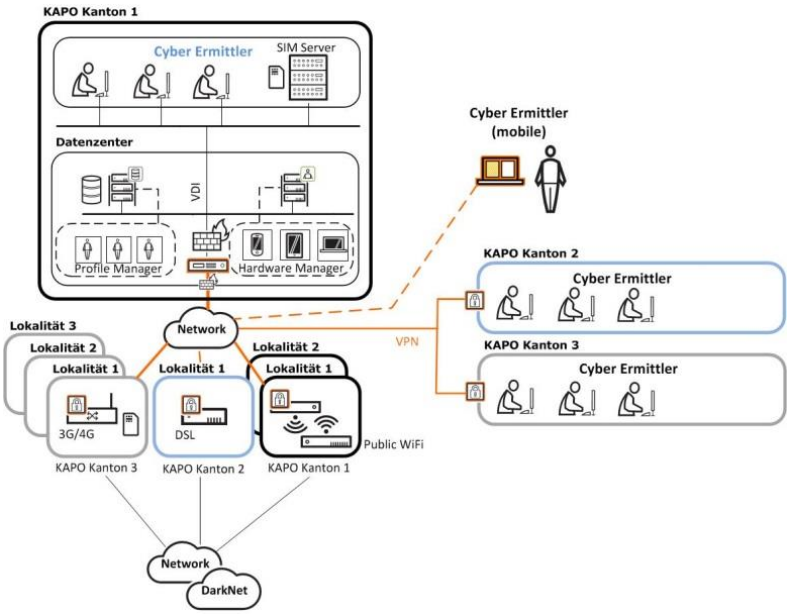


Abbildung 2: Mandantenfähigkeit des MINA-Systems



Zentrales Element des MINA-Systems ist die Profile- und Hardware-Manager-Einheit, welche für die Zusammenstellung und die Aufrechterhaltung der Tarnidentitäten verantwortlich ist. Zusätzlich wird dort die konsistente Hardware-Verwendung geregelt. Dies sowohl gegenüber den Ermittlern (intern) wie auch gegenüber dem öffentlichen Netz (extern).

Zudem werden von dort aus die verschiedenen Proxy-Zugänge an den externen Lokalitäten geregelt. Als Möglichkeit für den Zugang ins öffentliche Netz stehen GSM-Datengateways, DSL-Modems und WiFi-Gateways zur Verfügung.

Für den GSM-Datengateway ist optional ein zentraler SIM-Server vorgesehen. Mit dieser Option können die verwendeten Daten-SIM-Karten zentral verwaltet werden. Einerseits kann dadurch der betriebliche Aufwand verringert und können andererseits durch die konfigurierbaren IMEI der eingesetzten GSM-Gateways schnell neue mobile Profile erstellt werden oder existierende mobile Profile örtlich migriert werden.

MINA kann das föderalistische System nutzen
MINA soll mandantenfähig sein. Dadurch können Cyber-Ermittler aus verschiedenen Kantonen ein MINA-System zentral verwenden (siehe Abbildung 2). Während die betreibende Behörde z.B. lokal auf das Backend-System zugreifen kann, verbinden sich die Partnerbehörden aus den anderen Kantonen geschützt über das öffentliche Netz. Andererseits können die Partner den anderen Behörden aber entsprechende Lokalitäten für die Zugangsproxies zur Verfügung stellen.

Dadurch wird die Diversität der Tarnprofile infolge der der unterschiedlichen geografischen Lokalitäten der MINA-Internetzugangspunkte verbessert, was die Sicherheit für Cyber-Strafermittlungen massgebend erhöhen kann.

Falls dies möglich und gewünscht wird, können einzelne Proxies sogar bei Strafverfolgungs-behörden fallbezogen im Ausland stehen. So kann jeder Partner etwas zum optimalen Betrieb beisteuern – ein Riesenvorteil unseres Föderalismus!