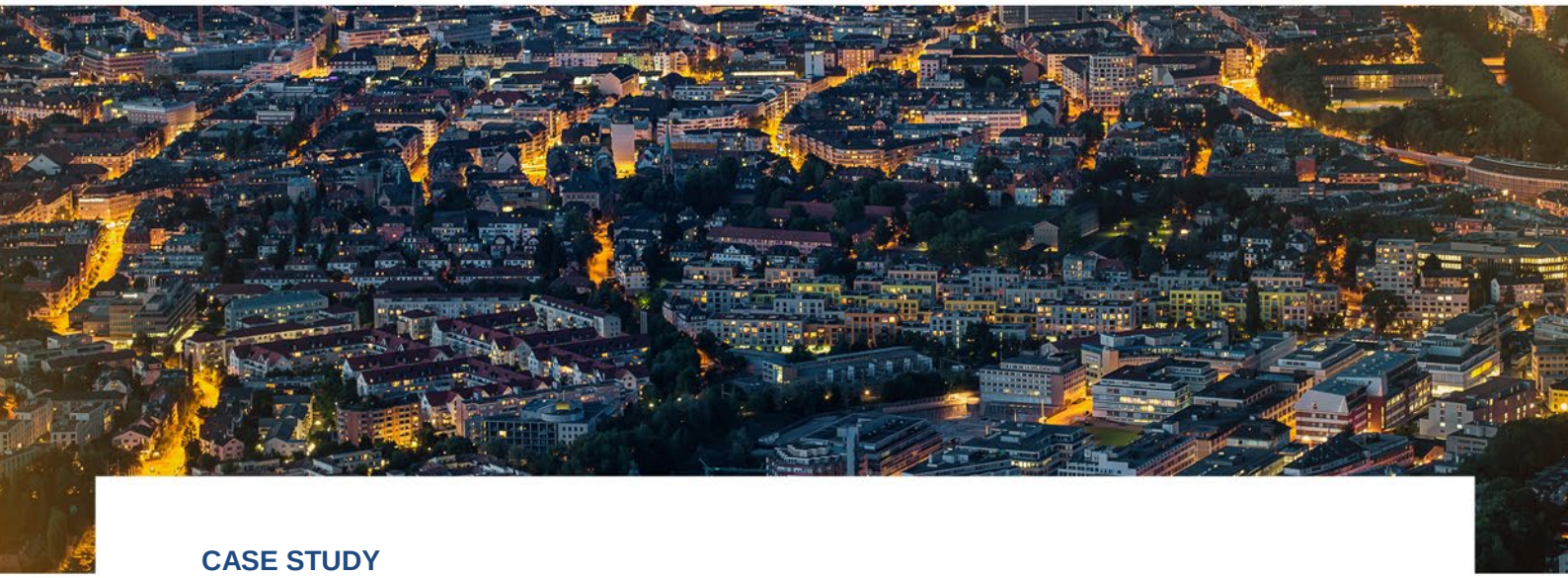
CyOne Security AG
Hinterbergstrasse 18
6312 Steinhausen

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



CASE STUDY

# Multi Identity Network Access (MINA)

## Wie sich Cyberermittler mit verschiedenen Tarnidentitäten konsistent im Internet bewegen können.

**Eine grosse Herausforderung für Cyberermittler ist es, sich unauffällig und konsistent im Internet und innerhalb des Dark-Webs bewegen zu können: Von ihrem Ermittlerarbeitsplatz aus, welcher eingebettet in einem Verwaltungsumfeld (Bund oder Kanton) ist bzw. von ihrem Arbeitsumfeld aus, sollen die Ermittler Täter im Netz identifizieren und cyberkriminelle Tätigkeiten bekämpfen.**

**Eines ist klar: Professionelle Cyberkriminelle agieren im Internet und im Dark-Web immer vorsichtiger und prüfen immer öfters ihre jeweiligen Kommunikationspartner oder Besucher sehr gründlich. So werden IP-Adressen, User-Agents, Cookies, verwendete Kreditkarten, Social-Media-Einträge etc. sorgfältig überprüft. Eine kleine Inkonsistenz und Misstrauen wird 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, welche keine verräterischen inkonsistenten Spuren im Netz hinterlassen.**

**Mit MINA (Multi Identity Network Access) will die CyOne Security einen Lösungsansatz aufzeigen, um die Cyberermittlung in ihren Herausforderungen zukünftig unterstützen zu können.**

**Herausforderung Netzidentität**
Für eine effektive Cyberermittlung ist es unter anderem wichtig, sich unauffällig und konsistent im Internet und innerhalb des Dark-Webs bewegen zu können. Problematisch wird es, wenn die Ermittler dies heute von ihrem Arbeitsplatz aus ohne entsprechende Werkzeuge durchführen 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 und in einem Starbucks-Kaffee mit öffentlich zugänglichem Wireless-Zugang einigermassen anonym ins Internet zu gehen, kann nicht die Lösung sein.

Werden 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, welcher die verschiedenen Sicherheitsbehörden von Kanton und Bund und den dort tätigen Cyber-Ermittlern zukünftig in der Bekämpfung von Cyberkriminalität unterstützen kann – von ihren jeweiligen Arbeitsplätzen aus.

MINA soll für die Cyber-Ermittler dabei nachfolgende Funktionen bereitstellen:

- Der Ermittler kann sich vorgängig aus verschiedenen Benutzerprofilen, Betriebssystemen und Hardwareprofilen passende Tarnidentitäten zusammenzustellen.
- Fallbezogen und konsistent kann er die definierten Tarnidentitäten einfach anwenden.
- Konsistent heisst dabei:
    - Anwendung der vordefinierten Hardware-Parameter gegenüber dem Internet-Service Provider und Telekom-Service Provider, gegenüber den Servern, Social-Network-Community und den Zielgruppen (z.B. verschiedene Betriebssysteme, User-Agent, MAC-Adressen, IMEI etc.).
    - Anzeigen der notwendigen Tarnidentität-Metadaten (z.B. Personalien, Email, Social-Media Accounts etc.) während der Ermittlung, um Fehlerraten zu verkleinern.
- Sichere, lückenlose und fallbezogene Speicherung der durchgeführten Ermittlungs-tätigkeiten.
- Verschiedene Betriebssysteme emulieren (Windows, Macintosh, Android, iOS).
- Unterschiedliche, konfigurierbare und geografisch getrennte eigene Proxy-Zugänge benutzen. Dies 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 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 gezügelt 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 verwendetet Profil wie auch die anfallenden Ermittlerdaten bleiben durch eine hohe Isolierung, bei der entsprechenden ermittelnden Behörde.
- Schnittstelle für einen sicheren Datenimport und -export in ein klassifiziertes Behördennetz (kompatible zu CyOne-Datenschleuse).
- Sicherer Remote-Zugriff auf MINA-Infrastruktur für mobile Cyber-Ermittler (Roadrunner-Ansatz) ermöglicht.

**MINA-Architektur**

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

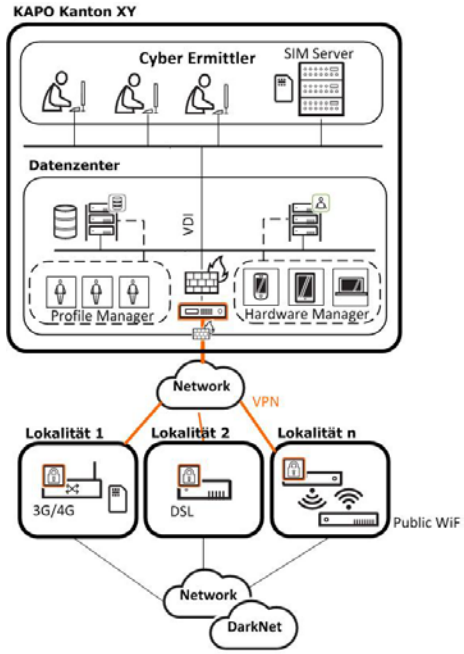



*Abbildung 1: schematische MINA-Architektur*

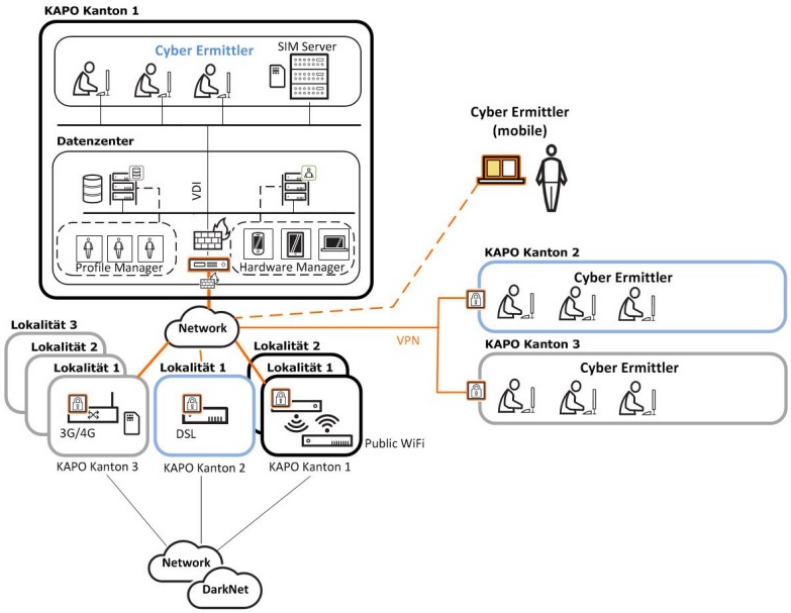



*Abbildung 2: Mandantenfähigkeit des MINA-Systems*

Zentrales Element des MINA-Systems ist die Profile- und Hardware-Manager Einheit. Diese ist für die Zusammenstellung und die Aufrechterhaltung der Tarnidentitäten verantwortlich. 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. Durch diese Option können die verwendeten Daten-SIM-Karten zentral verwaltet werden. Dies verkleinert einerseits den betrieblichen Aufwand und andererseits können durch die konfigurierbaren IMEI der eingesetzten GSM-Gateways schnell neue mobile Profile erstellt werden oder existierende mobile Profile örtlich gezügelt 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 aber entsprechende Lokalitäten für die Zugangsproxies den anderen Behörden zur Verfügung stellen.

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

Falls dies möglich und gewünscht wird, können einzelne Proxies sogar bei Strafverfolgungsbehörden fallbezogen im Ausland stehen. So kann jeder Partner etwas für den optimalen Betrieb beisteuern -  ein riesen Vorteil unseres Föderalismus!