PUBLIC

MINA & Co:

«Plattform für repressive und präventive Cyber-Ermittlungen»

SPIK-Event 2021

Stefan Frank, Senior Security Consultant

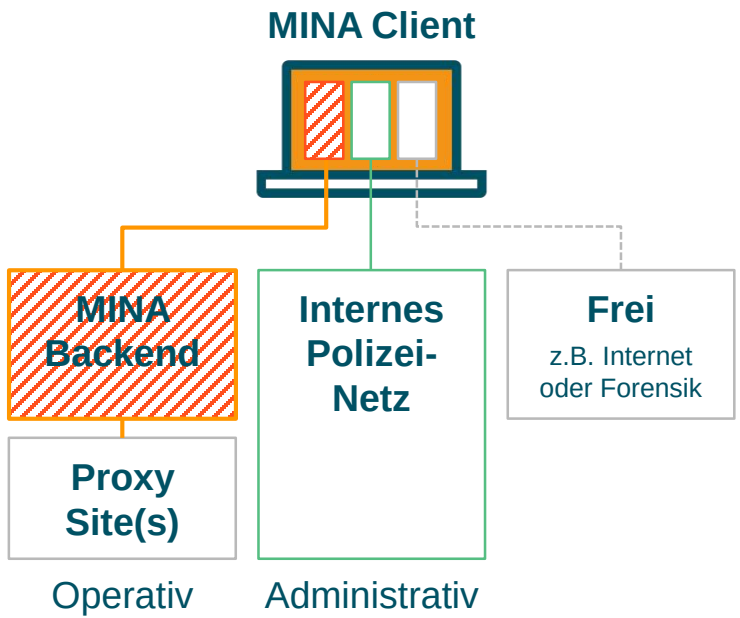
Bern, 11. Mai 2021

Agenda

01 – CyOne Security Vision «MINA»
02 – MINA: Architekturübersicht
03 – Demo

01 – CyOne Security Vision «MINA»

Was ist MINA?



MINA:
Multi **I**dentity **N**etwork **A**ccess

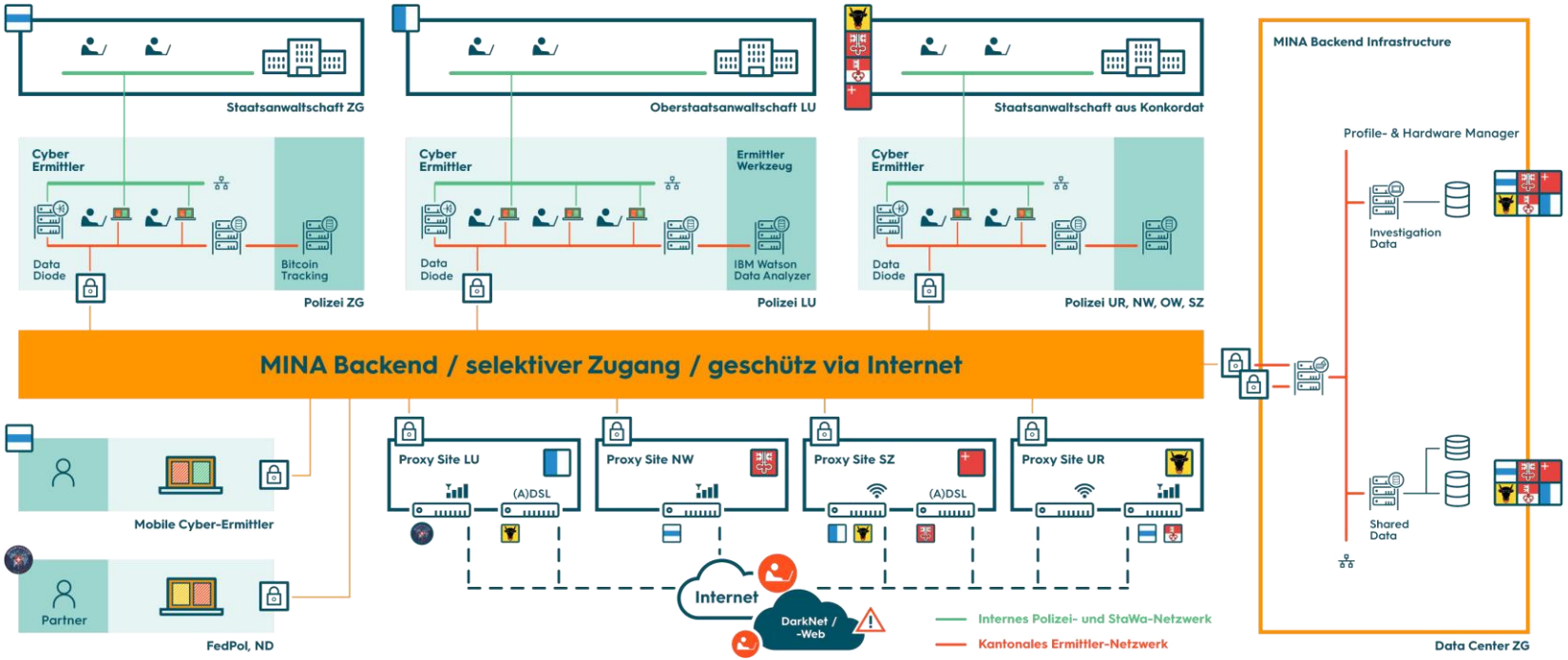
Erlaubt Cyber-Ermittlern von **einem einzigen Endgerät** aus auf verschiedene Infrastrukturen (Zonen) sicher zuzugreifen (max. 4).

Ermöglicht anonyme oder legendierte Bekämpfung von Internetkriminalität. Dafür stehen definierbare Hardware- und Benutzerprofile fallbezogen zur Verfügung.

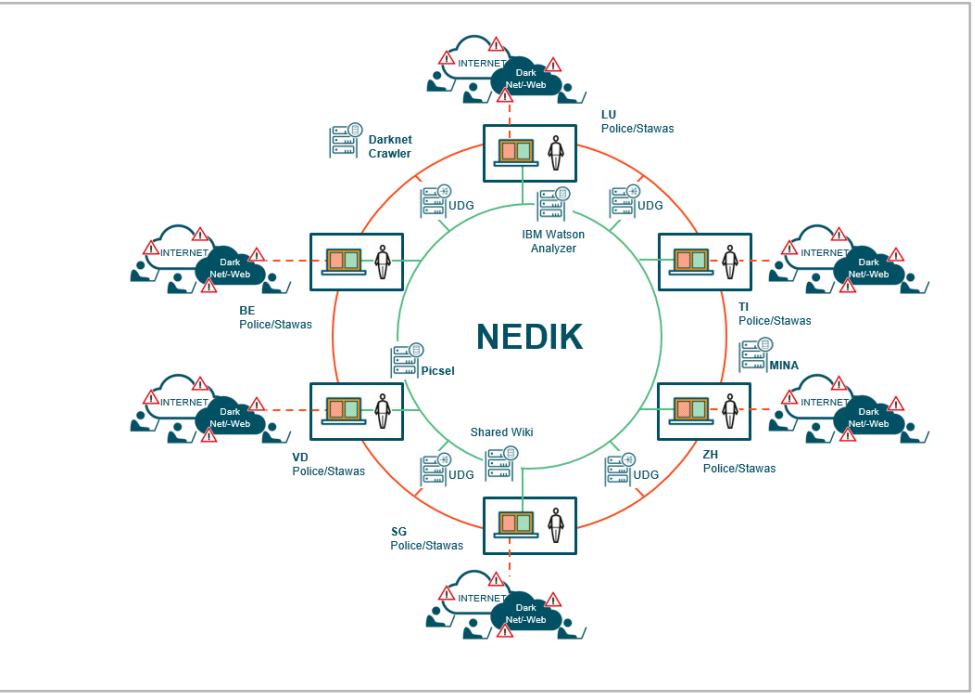
Operative Erkenntnisse und relevante Daten können ins interne Polizei-Netzwerk **sicher importiert** werden.

Polizeikorp übergreifend können im operativen Ermittlerumfeld auf vorhandene Internetzugänge (Proxy Sites) und auf OSIF-Daten zugegriffen werden.

Unsere Vision



Erweiterung von NEDIK?



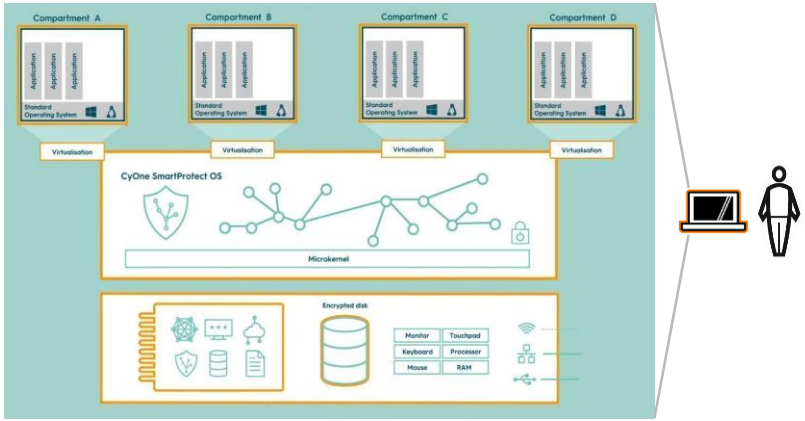
Mit NEDIK verfügen die Cyber-Ermittler der Polizeikorps über ein Netzwerk für den Wissenstransfer, eine Fallübersicht, die Triage und die Koordination.

Mit MINA wird dieses Netzwerk operativ erweitert durch:

- Eine Bündelung der «operativen Einsatzmittel» für die Bekämpfung der digitalen Kriminalität
- Eine grössere Zugangs-Diversität für verdeckte Fahndungen und Informationsbeschaffungen im digitalen Raum
- Eine höhere Cyber-Resilienz des Ermittler-Endgerätes (durch höchste Isolierung)
- Eine Reduktion der Arbeitsinstrumente für die Cyber-Ermittler

02 – MINA: Architekturübersicht

MINA Client



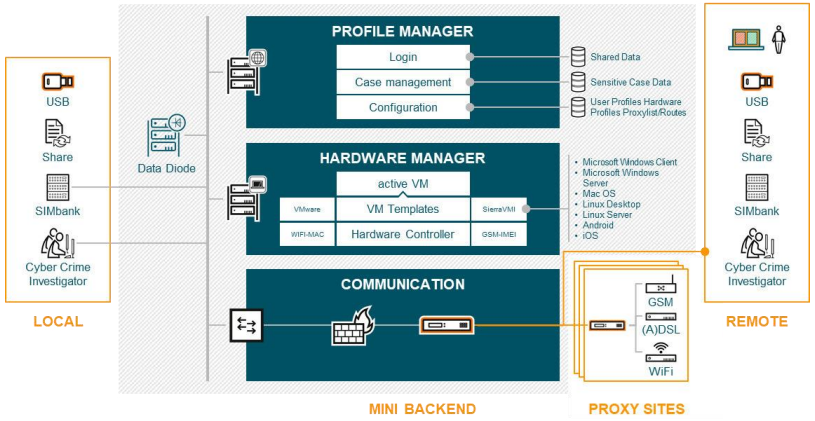
CyOne SmartProtect Security Module, welches das Boot-Image des CyOne SmartProtect OS sowie die Chiffrier- und Authentifizierungsservices enthält.

Das Microkernel-basierte **CyOne SmartProtect OS,** welches über eine unveränderbare Sicherheits-architektur verfügt.

Dieses sichere OS stellt die **komplette Isolation** der virtualisierten Benutzerumgebungen (Compartments) sicher.

Dabei wird sichergestellt, dass bei einer unbeab-sichtigten Malware-Infektion oder bei einem Cyber-Angriff, der **Sicherheitsvorfall in der entsprechenden Zone isoliert bleibt.**

MINA Backend-Konzept



Die ganze Konfigurationen und das Fallmanagement (inkl. Daten) soll über einen **Profile Manager** ausgeführt werden.

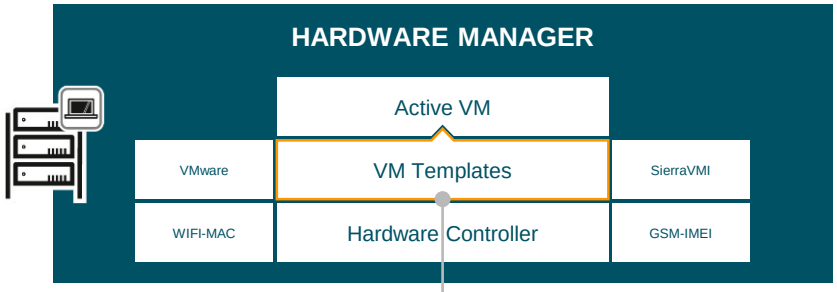
Ein **Hardware Manager** soll alle VM Templates (Client-, Server- und Mobile-Images) sowie den Hardware Controller beinhalten.

Jedes «Legenden»-Userprofile soll bis zu 3 Hardwareprofile haben können.

Es soll sowohl die MAC-Adresse (Notebooks, Desktops und Server) als auch IMEI-Adresse (Android, iOS) verändert werden können.

Eine **Kommunikation Einheit** soll für das entsprechende Routing verantwortlich sein (Remote Polizeikorps und Proxy Sites).

Beispiel: Mögliche Ausprägung



VM1
Tails / TOR

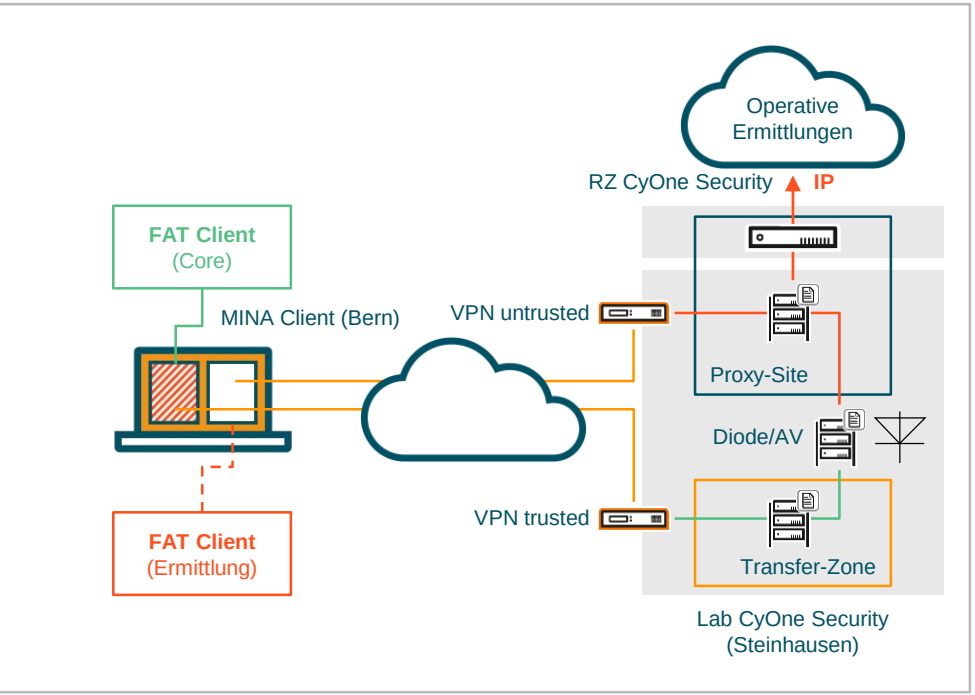
VM2
Cryptowährung-Tracking

VM3
Mobile App

VMn
Server für Web-Crawler

03 – DEMO

Demo-Setup



MINA Client mit 2 Compartment

- Core: Arbeitsumgebung (FAT Windows 10)
- Ermittlung: Ermittlungsumgebung (FAT Ubuntu 18.04)

Pro Compartment geschützte Verbindung in das Lab von CyOne Security (in Steinhausen).

Zugang ins Internet über dezidierte IP-Adresse Proxy-Site (RZ von CyOne Security).

CORE Zone isoliert.

Datenimport möglich via Diode in Transfer-Zone.

RDP-Zugang auf Transfer-Zone (inkl. copy/paste)

Sichere Schweiz.
Bit für Bit.

Jetzt Live Demo bei Ihnen vor Ort anfordern!

Stefan Frank
Senior Security Consultant
Email: stefan.frank@cyone.ch
Phone: +41 41 748 85 61

cyone.ch

BLOG Cyber Security BLOG IoT Security