Öffentliche Präsentation

«Sichere und wirtschaftliche Kollaboration im Cyber- und Lageverbund»

SPIK 2022

Reto Amstad, Senior Security Consultant

Bern, 06. April 2022

Agenda

01 – «Cyber-Black-Friday» – Herausforderungen für eine sichere Kollaboration
02 – Anforderungen an einen resilienten Lageverbund
03 – Architekturübersicht «Resilienter Lageverbund»
04 – Fragen und Diskussion

SPIK 2022

«Cyber-Black-Friday»

Herausforderungen für eine sichere Kollaboration

«Cyber-Black-Friday»?

Pressemitteilungen 07. April 2023

- Grossflächiger Cyber-Angriff auf Detailhandel: Migros, COOP, Aldi etc.
- Verteilzentren sind durch Ransomware stillgelegt. Es wird nur wenig Ware ausgeliefert.
- Weitere Industrieunternehmen sind betroffen.
- Öffentliche Verwaltungen sind ebenfalls nur teilweise operationsfähig.

Nach 2 Tagen

- Das Problem ist noch nicht gelöst.
- Die Ware staut sich in und vor den Verteilzentren.
- Die Regale in den Läden leeren sich.

Nach 3 Tagen

- Es kommt zu Plünderungen und ersten gewalttägigen Auseinandersetzungen.
- Behörden müssen bei der Verteilung von Lebensmitteln unterstützen.

Ist die Schweiz mit der NCS 2.0 dagegen gewappnet?

SPIK 2022

Anforderungen an einen resilienten Lageverbund

Strategische Ziele NCS 2018-2022

«Die Schweiz ist gegenüber Cyber-Risiken resilient. Die Fähigkeit der Kritischen Infrastrukturen, wichtige Dienstleistungen und Güter zur Verfügung zu stellen, bleibt auch bei grossen Cyber-Vorfällen gewährleistet.»

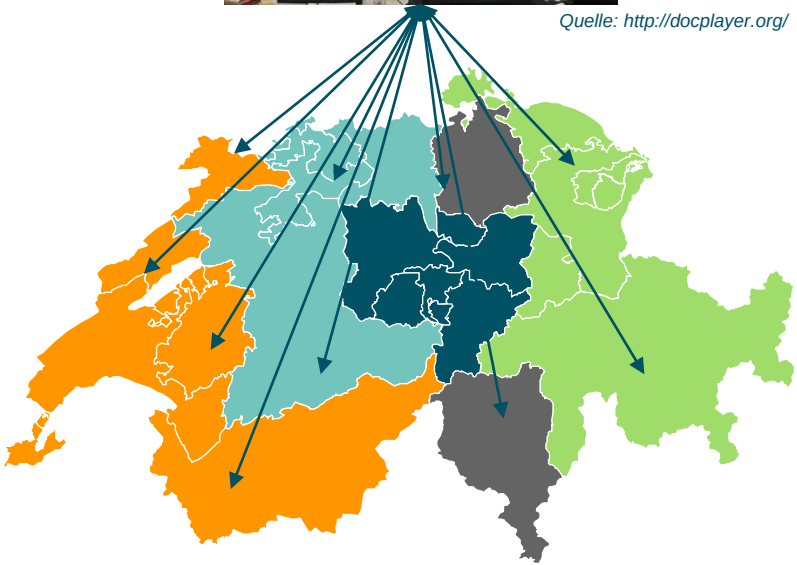
«Die Schweiz verfügt in allen Lagen über die nötigen Kapazitäten und Organisationsstrukturen, um Cyber-Vorfälle rasch zu erkennen und auch dann zu bewältigen, wenn diese über längere Zeit andauern und verschiedene Bereiche gleichzeitig betreffen.»

Quelle: Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018–2022

Herausforderungen «Sicherer Lageverbund»

- Kollaborationsdruck unter den Behörden (national wie international)
- Heterogene Infrastruktur und SW-Landschaft der verschiedenen Behörden und Kantone
- Cybercrime: zunehmende Bedrohung für Behörden und Kritische Infrastrukturen
- Risiken aus der Supply Chain nehmen zu
- Fachkräftemangel und Budgetdruck

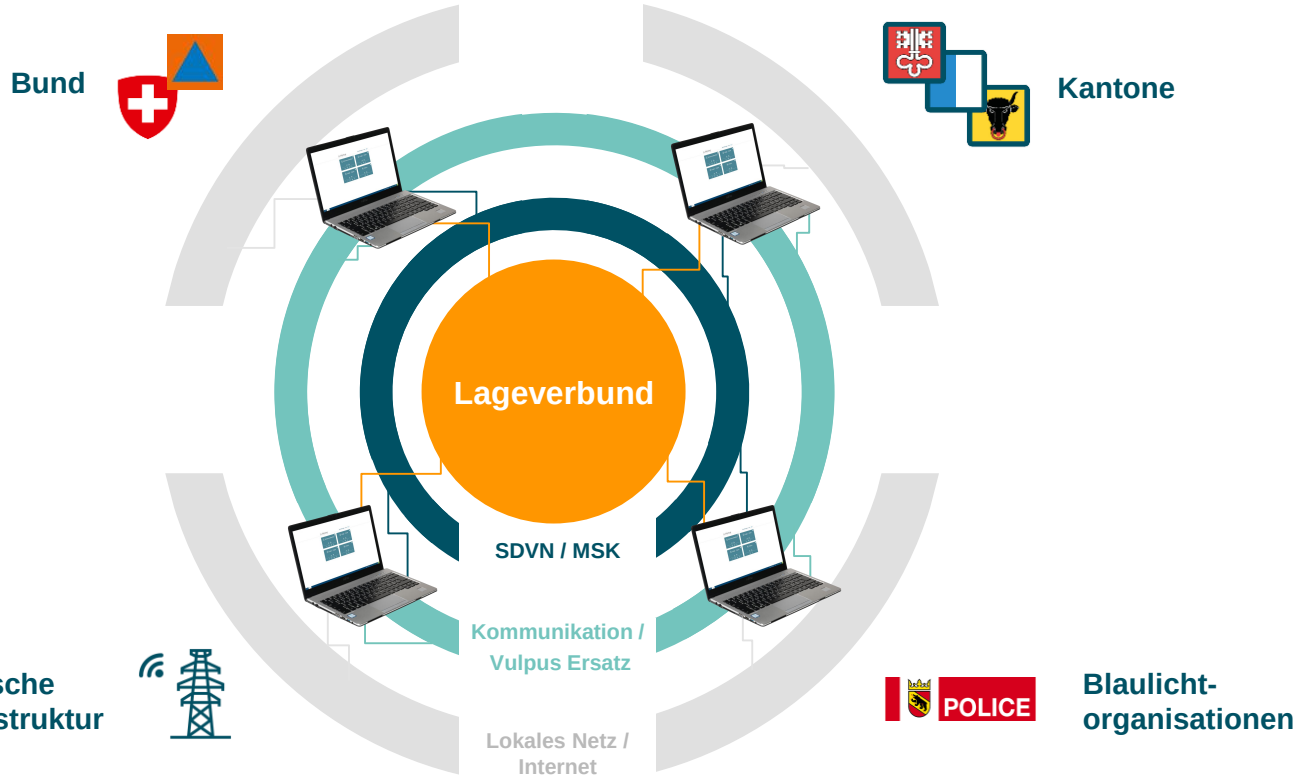
Quelle: http://docplayer.org/



SPIK 2022

Architekturübersicht «Resilienter Lageverbund»

Lageverbund – viele Schnittstellen

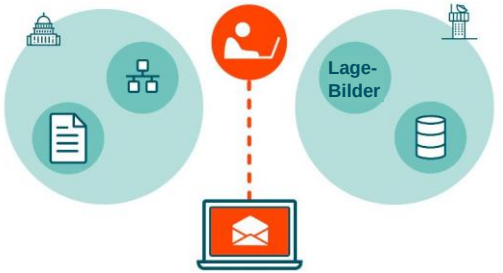


«Endpoint Security»: wichtiger denn je

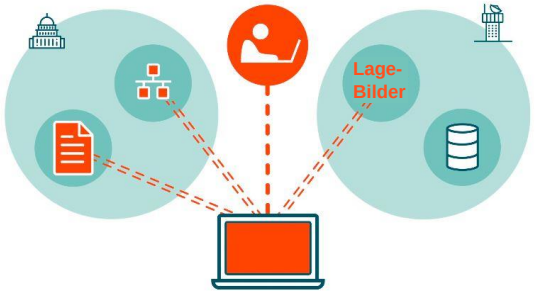
- «Endpoint Security» beschreibt die Sicherung von Endpunkten und Endbenutzergeräten.
- Endbenutzergeräte müssen heute Zugriff auf verschiedene Netzwerkzonen haben (barrierefreies Arbeiten).
- Bei einem erfolgreichen Angriff auf ein Endgerät (1) können dadurch die verschiedenen Netzwerkzonen auch durch eine Malware kompromittiert werden (2).

Endgerät-Sicherheit ist darum heute wichtiger denn je!

1 **Angriff auf Endgerät**



2 **Infektion der Netzwerkzonen**



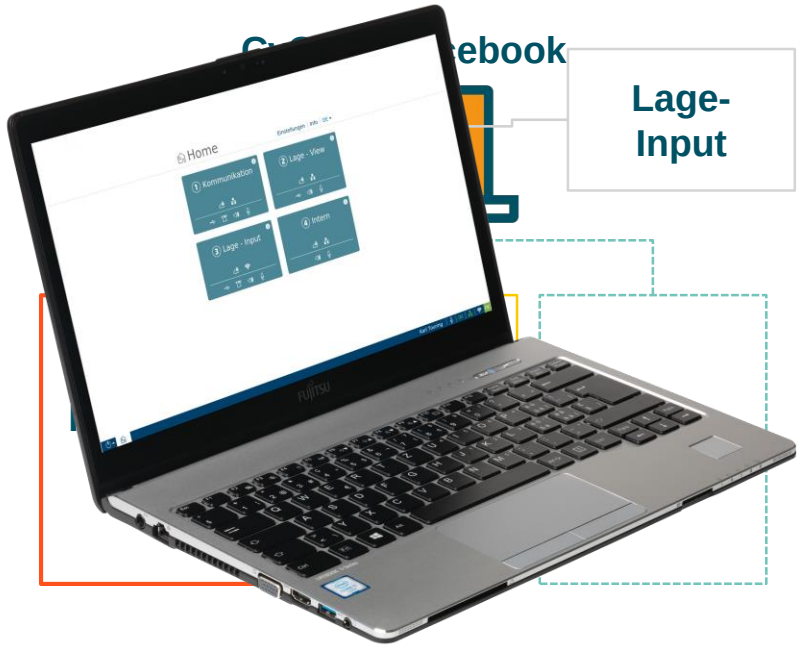
Lösungsansatz: «Sichere Isolation»

«CyOne Officebook»
mit «CyOne SmartProtect Technology»
(Swiss made)

- Um die Cyber-Risiken für das Benutzerendgerät zu eliminieren und effizientes Arbeiten in einer vernetzten Arbeitswelt zu ermöglichen, hat die CyOne Security **für Schweizer Behörden** die **«SmartProtect Technology»** entwickelt, welche:
- unterschiedliche Benutzerumgebung sicher voneinander trennt;
- einen geschützten isolierten Netzwerkzugang in eine oder mehrere vordefinierte (Sicherheit)-Zone(n) ermöglicht;
- komfortables Arbeiten in verschiedenen Benutzerumgebungen erlaubt.

Dies alles mit einem einzigen Endgerät!

CyOne Officebook im Lageverbund



CyOne Officebook

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

Kommunikation: Es ermöglicht neben einer Videokonferenz auch den zur Kollaboration notwendigen Austausch von Daten (z.B. E-Mail, Chat etc.).

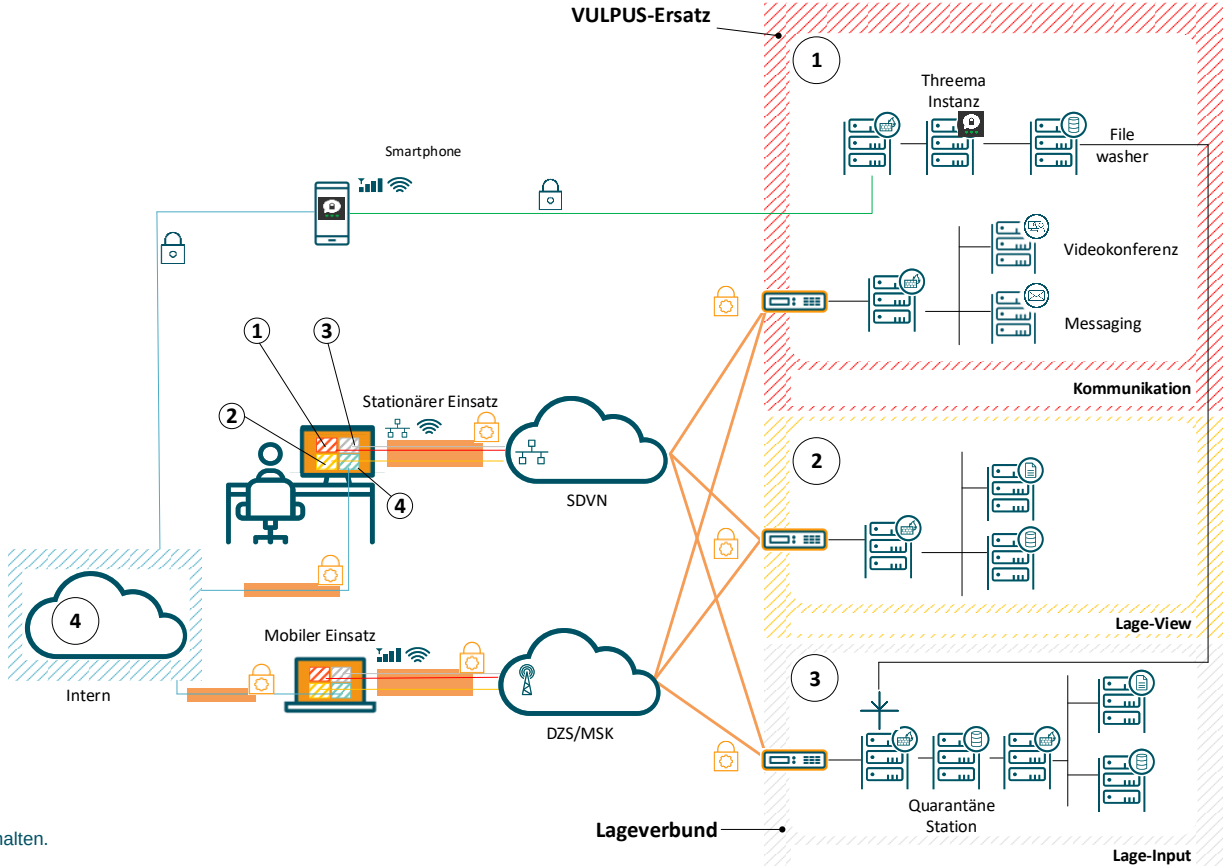
Lagedarstellung (View): Hier werden alle aufbereiteten Daten als nutzbares Lagebild dargestellt.

Lagebearbeitung (Input): Dies stellt die eigentliche Schnittstelle für die Eingabe aller für die Lage relevanten Daten dar.

Intern / bestehende Behörden IT: stellt die Einbindung in die bestehende IT-Infrastruktur der entspr. Behörde dar.

Übersicht Einsatz im Lageverbund

- Sicherer Zugriff auf mehrere Zonen
- Zentrales und sicheres Management der Clients
- Integration von Mobile-Applikationen in der Gesamtlösung
- Unkomplizierte Integration in heterogene Behördenlandschaft
- Höchste Sicherheit des Endgeräts und der Kommunikation
- Erprobte Lösung im Behördenumfeld



Sichere Schweiz.
Bit für Bit.

CyOne SECURITY

Vielen Dank für Ihre Aufmerksamkeit!

Reto Amstad
Senior Security Consultant
Email: reto.amstad@cyone.ch
Phone: +41 79 723 18 41

cyone.ch

BLOG Cyber Security

BLOG IoT Security