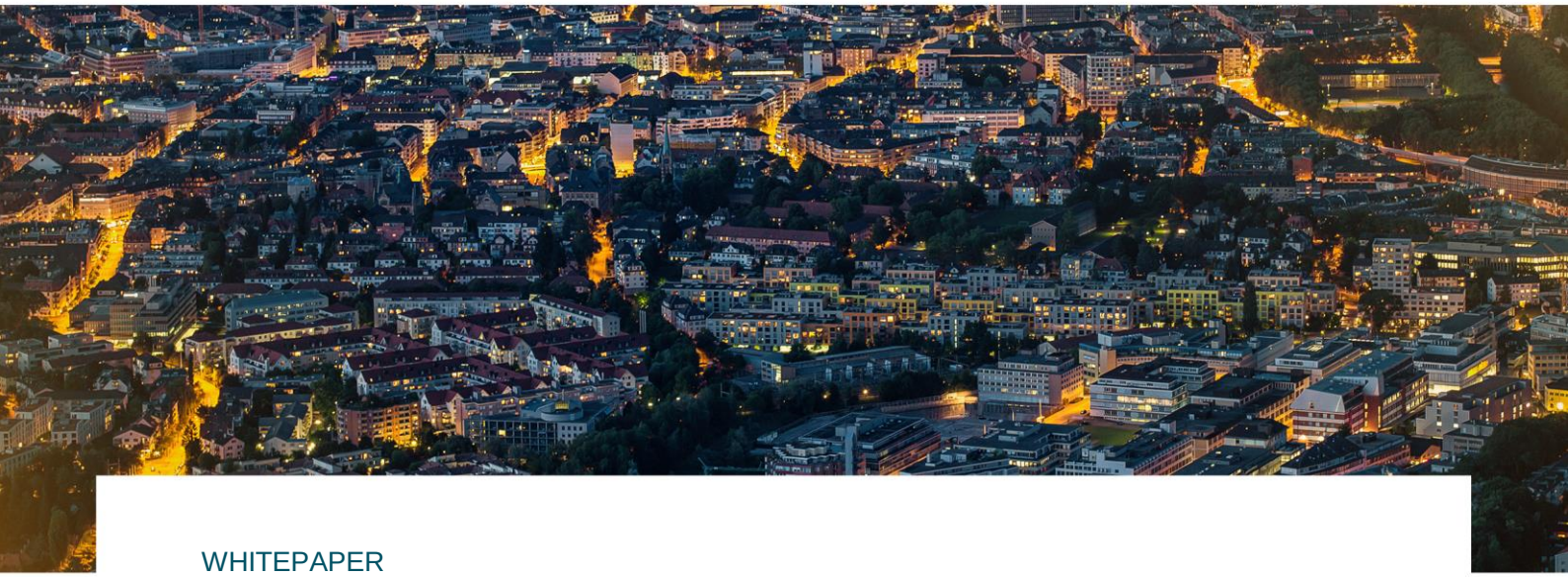
CyOne Security AG
Hinterbergstrasse 18
6312 Steinhausen

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



WHITEPAPER

CyOne Workplace System: Sicheres mobiles Arbeiten auch in Krisensituationen

Roland Odermatt | Leiter Verkauf Behörden | Steinhausen, 21. Dezember 2021

Digitale, mobile Arbeitsplätze sind im Behördenumfeld – gerade in Krisensituationen – unabdingbar. Die eingesetzten spezifischen Cyber-Security-Lösungen müssen benutzerfreundlich sein und jederzeit den zeitnahen, sicheren Zugriff auf sensible Daten von allen Standorten aus garantieren.

Krisensituationen wie beispielsweise eine grassierende Pandemie können mit massiven Mobilitätseinschränkungen verbunden sein. Unerlässlich sind deshalb sichere Lösungen, die abseits des Verwaltungsbüros Zugriff auf ihre gewohnte Arbeitsumgebung, Fachapplikationen und ihre Dokumente erlauben. Im Spannungsfeld Sicherheit versus Benutzerkonformität geht es für die verantwortlichen Sicherheitsarchitekten der Behörden darum, geeignete Arbeitsmittel und Plattformen bereitzustellen. Diese müssen sich in einer von Cyber-Attacken geprägten Umgebung beziehungsweise einer sich permanent ändernden Bedrohungslage behaupten können.

Endgeräte sind bevorzugte Einfallstore für Cyber-Kriminelle

Grundsätzlich sind Endgeräte heute immer noch eines der bevorzugten Einfallstore der Cyber-Kriminellen. Am Arbeitsplatz, wo die sensiblen Daten bearbeitet werden, können sie entwendet oder modifiziert werden. Dabei werden häufig Angriffsvektoren über den Benutzer als Einfallstor gefahren. Bei E-Mail (Phishing) oder klassischen USB-Sticks (Baiting) wird eine Unachtsamkeit des Benutzers ausgenutzt, um in das Behörden-Netzwerk zu gelangen.

Die Risiken für die geforderten modernen mobilen Arbeitsinstrumente sind durch Exponieren der betreffenden Endgeräte noch um ein Vielfaches höher. Dies weil einerseits das betreffende Endgerät nicht mehr im IKT-Schutzperimeter mit Firewalls, IDS/IDP etc. ist. Andererseits sind die Endgeräte ja auch ausserhalb des physischen Sicherheitsperimeters und dadurch fallen auch die üblichen Zutrittsbeschränkungen zu Gebäuden oder den einzelnen Büros weg. Im Remote-Betrieb fehlen überwachte Zugänge (Logen-Betrieb), Videoüberwachungen oder die strikt geregelten Zutrittsberechtigungen gänzlich. Dies erfordert eine zusätzliche Härtung der Plattform, um die fehlende kontrollierte Umgebung zu kompensieren.

Herausforderung: die Netzübergänge der verschiedenen Sicherheitszonen

Risikomitigierend werden dafür in der Infrastruktur spezielle Netzwerkübergänge geschaffen. Ein mobiler Nutzer landet dabei zuerst auf einer Remote Access Zone, hat initial wenig Rechte und dadurch einen limitierten Zugang zu sensitiven Daten. Erst wenn er und die Plattform authentifiziert worden sind, wird dem Gerät der Zugang zu einer höheren Sicherheitszone gewährt. Die entsprechenden Netzübergänge sicher zu realisieren und gegenüber den sich wandelnden Cyber-Bedrohungen aktuell zu halten, stellt dabei eine grosse Herausforderung für die verantwortlichen IKT-Infrastrukturbetreiber dar.

Für Organisationen innerhalb der Verwaltungen, welche sensible Daten verwalten müssen, stellt diese Zonierung eine zusätzliche Herausforderung und einen Mehraufwand beim Betrieb dar. Diese Verwaltungseinheiten brauchen einen hohen Schutz, der aber nicht auf Kosten der Benutzerfreundlichkeit gehen darf. Die hier zum Einsatz kommende Cyber Security muss deshalb zuverlässig und benutzerfreundlich zugleich sein. Ansonsten können die Arbeiten von unterwegs nicht effizient erledigt werden und die Nutzer wenden die Sicherheit nicht konsequent an Zu oft wurden in der Vergangenheit auch in der Verwaltung benutzerunfreundliche Sicherheitsprozesse durch unzufriedene Mitarbeitende durch eine Schatten-IT mit Dokumentenkopien auf USB-Sticks oder gar Cloud-Speicher ersetzt. Auf diese Weise wird anstelle einer besseren Cyber-Resilienz das gesamte Sicherheitssystem aufs Spiel gesetzt. Das lässt sich vermeiden, wenn die komplexen Prozesse, welche die Informationssicherheit gewährleisten, optimal im Hintergrund ablaufen.

Erfolgsfaktor: Ganzheitlicher «Cyber Defence in Depth»-Lösungsansatz

Standard-Referenzarchitekturen stossen im Behördenumfeld und im Umgang mit hochsensitiven Daten an ihre Grenzen. Eine erfolgreiche Cyber Defence bedingt in diesem Umfeld ein ganzheitlicher «Cyber Defence in Depth»-Ansatz, der die speziellen Anforderungen im Umgang mit hochsensiblen Daten zu erfüllen vermag.

Die fünf relevanten Massnahmen

1. Die klare Separation der Netzwerk- und Dateninfrastruktur in drei sicherheitstechnisch aufsteigende operative Zonen z.B. «Internet / Intern», «Vertraulich» und «Geheim». Diese einzelnen Zonen müssen klar definierte und überwachte Datenzugänge- und Datenübergänge in die jeweils sicherheitstechnisch höhere Zone aufweisen. Idealerweise werden die Übergänge zentral ausgeführt, sodass sie performant betrieben, überwacht und effizient gewartet werden können.

2. Elektronische Kennzeichnung von Datenobjekten als Grundlage für die Filterung und das richtige Routing an diesen Zonenübergängen (z.B. basierend auf IST-68/RTG-031 – XML in Cross-Domain Security Solutions).

3. Überwachung dieser drei Netzwerkzonen mit kommerziellen modernen Cyber Security-Produkten, welche eine Orchestrierung und eine schnelle Respond-Fähigkeit innerhalb eines zentralen Security Operation Center (SOC) erlauben. Die dafür notwendige cyber-relevante Datenaggregation und Auswertung sowie die Re-Alimentierungsfähigkeit aller Sicherheitskomponenten muss innerhalb einer hochisolierten und geschützten vierten Zone stattfinden (Cyber Defence-Zone).

4. Schaffung eines einzigen Endgerätes, das die Sicherheitsvorgaben der drei operativen Zonen strikt umsetzen kann und den mobilen Anforderungen des modernen Behördenmitarbeitenden gerecht werden kann.

5. Die Integration von klassischen Cyber Defence-Ansätzen.

«Cyber Defence in Depth» durch zentral gehaltene Netzwerkübergänge

Eine strikte Trennung der Betriebssysteme auf dem Client erhöht die Sicherheit auf dem Endgerät durch das Isolieren und Trennen von Arbeitsumgebungen. Damit ist jedoch ein effizientes Arbeiten in Zonen mit unterschiedlichen Klassifikationen nicht automatisch gelöst. Spätestens wenn Daten und Dokumente gedruckt und versendet oder importiert werden sollen, stellt sich die Herausforderung der geeigneten Zonenübergänge. Erst sie erlauben die übergreifende Kommunikation und den Datenaustausch und sind für eine effiziente und moderne Arbeitsweise notwendig.

Sicherheitstechnisch stellen genau diese Zonenübergänge eine grosse Herausforderung dar. Bei jedem dieser Übergänge muss streng und zuverlässig kontrolliert werden können, welche Daten und Inhalte passieren dürfen, und welche Inhalte die klar definierte Zone nicht verlassen dürfen. Zur Erhöhung der Cyber Security müssen dort zudem Daten, Dokumente und Protokolle konvertiert werden, um Schwachstellen der Datenformate und Übermittlungsprotokolle zu minimieren. Mit dieser Konvertierung werden allfällig sensible Metadaten eliminiert respektive standardisiert und ausserdem mögliche Viren beseitigt. Der Zonenübergang ist dabei als «Owner» verantwortlich für die initiale Klassifizierung der Daten und deren Überprüfung. Per Datentagging kann der Zonenübergang auch tiefer klassifizierte Daten innerhalb einer höheren Sicherheitszone verteilen und sicherstellen, dass diese Daten die Zone nur verlassen können, wenn sie nicht verändert wurden (z.B. durch Hashing). «Defence in Depth» auf einem zonierten Endgerät bedeutet also:

- Die notwendigen Funktionalitäten für ein effizientes Arbeiten müssen an den zentralen Zonenübergängen auch definiert werden.
- Die Übergänge in einer zentralen Infrastruktur müssen performant ausgelegt und die Administration und Überwachung zentral und dadurch effizient gehalten werden.

- Sämtliche Datenobjekte am Zonenübergang sind elektronisch zu kennzeichnen (Taggen), um sicherzustellen, dass Daten in eine höher klassifizierte Umgebung zuverlässig und sicher verteilt werden können.
- Die elektronische Kennzeichnung soll dazu dienen, einen (weiteren) Export in tiefer klassifizierte Zonen nur dann zu ermöglichen, wenn die Daten unverändert vorliegen resp. Änderungen an den Daten und tiefer klassifiziert festgestellt werden können.

CyOne Workplace System: strikte Trennung für maximale Sicherheit

Das Workplace System von CyOne Security löst den Zielkonflikt zwischen maximalem Schutz und grösstmöglichem Bedienkomfort. Durch eine sichere Aufteilung der Hardware in zwei oder mehrere Bereiche können Nutzer damit bequem auf öffentlich zugängliche Informationen im Internet zugreifen, ohne dabei die internen Informationen und die IT-Infrastruktur ihrer Organisation zu gefährden. Parallel dazu läuft der sichere Zugriff auf sensitive IT-Bereiche. Das System ist einfach konfigurierbar und lässt sich in die bestehende IT-Umgebung integrieren, indem bestehende Betriebssystemumgebungen virtualisiert werden und mit einer sicheren Hardwareplattform und sicheren Zugangselementen vollständig umschliessend geschützt sind.

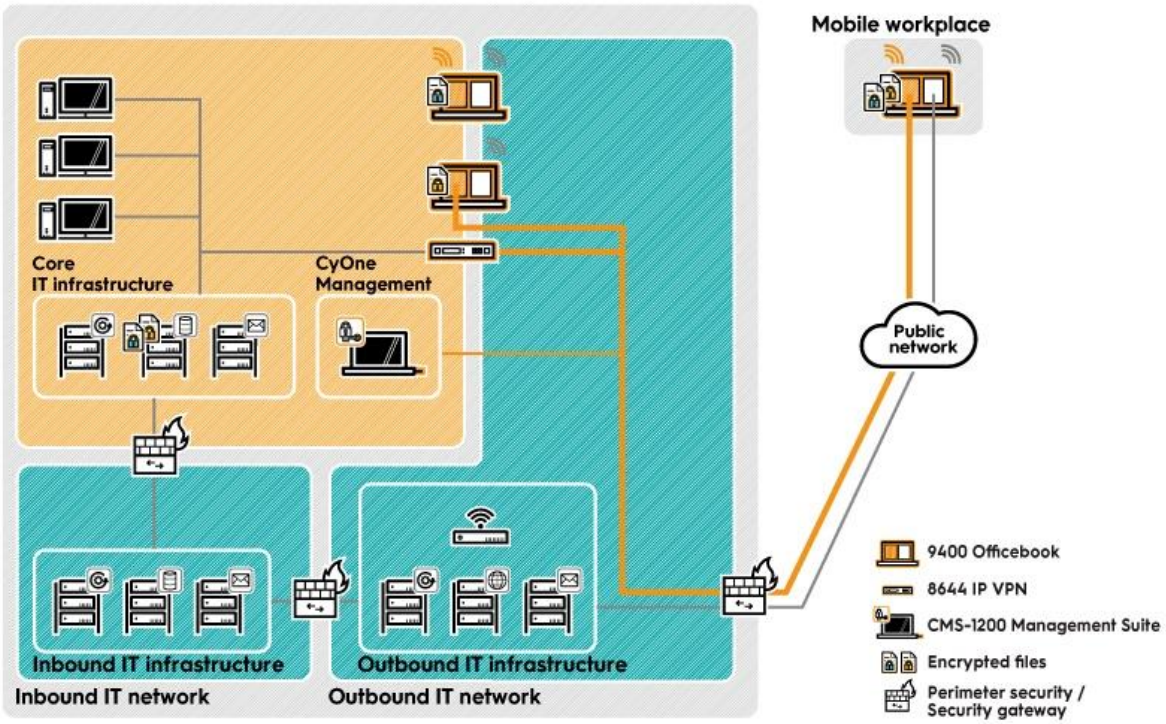
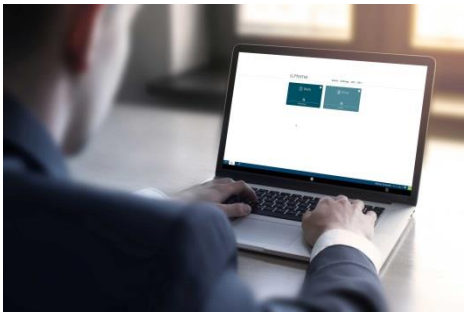


Abbildung 1 Schutz interner Informationen und der IT-Infrastruktur

Um ein Betriebssystem in einer sicheren virtuellen Umgebung zu betreiben, wird ein Sicherheitsbetriebssystem (Sicheres OS) benötigt, das die Hardware (Prozessor, Festplattenspeicher, RAM etc.) in sichere virtuelle Bereiche trennt, ohne dass dabei unerlaubte Zugriffe oder Zonenübergänge entstehen. Das Sicherheitsbetriebssystem seinerseits darf nicht angreifbar sein und schützt sich vor unerlaubten Zugriffen mit Mechanismen wie Secure Boot, Secure Update und starker Authentifizierung. Für den Nutzer ist die Sicherheit unbemerkt im Hintergrund. Die zwei oder mehrere vollständig voneinander getrennte Compartments (Benutzerumgebungen) auf dem 9400 Officebook stellen sich wie zwei Fenster dar, in welchen parallel gearbeitet werden kann.



So können mit der einen Benutzerumgebung sensible interne Informationen bearbeitet werden. Diese Umgebung verbindet sich über eine gesicherte Verbindung mit der IT-Infrastruktur der Behörde und ermöglicht den Online-Zugriff auf zentrale Informationen und Applikationen. Mit der zweiten Benutzerumgebung kann sich der Nutzer mit öffentlichen Netzen verbinden und damit auch auf öffentlich verfügbare Informationen zugreifen. Beide Compartments können gleichzeitig betrieben werden, der Wechsel vom einen zum anderen erfolgt über einen einfachen Klick.

Mehrwert für Mitarbeitende und Sicherheitsverantwortliche

Dadurch erhalten Behördenmitarbeitende uneingeschränkte, sichere Mobilität und können so ortsunabhängig, vernetzt und effizient arbeiten – zum Beispiel ist Home Office in Zeiten einer Pandemie eine verbreitete Massnahme zur Infektionsprävention. Als Sicherheitsverantwortliche erhalten Sie eine nachhaltige Cyber-Defence-in-Depth-Lösung, welche hilft, die Auswirkungen einer möglichen Cyber-Attacke auf die IT-Infrastruktur Ihrer Organisation zu minimieren. Durch die Härtung des Endgeräts kann der Netzübergang allenfalls einfach gehalten werden. Dies erspart Betriebskosten und Personalaufwand für den Betrieb eines komplexen Sicherheitsübergangs.

Beginnen Sie heute, Ihre Organisation auch während einer Pandemie vor Cyber-Risiken zu schützen, damit Ihre Mitarbeitenden jederzeit und überall sicher und vernetzt arbeiten können.

Machen Sie den ersten Schritt: Analysieren Sie gemeinsam mit unseren Experten Ihre aktuellen und zukünftigen Cyber-Sicherheitsbedürfnisse und entsprechende Sicherheitslösungen.

Kontaktieren Sie uns für ein kostenloses Expertengespräch.