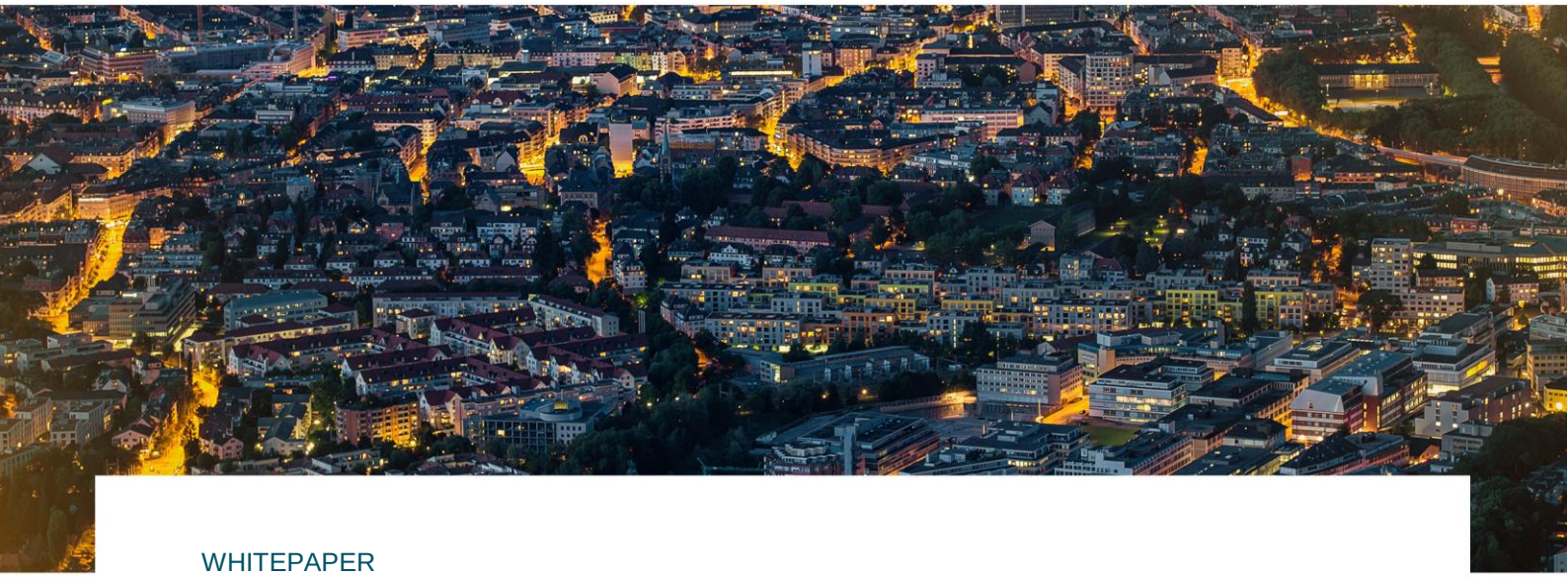
CyOne Security AG
Hinterbergstrasse 18
6312 Steinhausen

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



WHITEPAPER

Datensicherheit für verschiedene Rollen – durch konsequente Zonentrennung

Beat Püntener | Productmanager | Steinhausen, 23. November 2021

Politikerinnen und Politiker sind in der Schweiz durch das einzigartige politische Milizsystem besonders exponiert: Sie alle sind Amts-, Privat- und Geschäftspersonen in einem. Wer ständig zwischen Amtsstube, Büro und Zuhause hin- und herpendelt, nutzt aus Bequemlichkeit oft nur einen Laptop beziehungsweise nur ein Smartphone – folglich sind auch Daten aus allen drei Sphären auf dem gleichen Gerät gespeichert.

Ebenfalls ist die Präsenz auf den Social Media quasi eine Notwendigkeit. Die Amtspersonen exponieren sich durch ihre digitalen Devices über die Accounts von Social Media. So können die benutzten Geräte wie Smartphones, Tablets und Laptops als Einfallstor zu privaten und geschäftlichen sowie zu IT-Systemen von Behörden dienen.

Die Ansprüche an Rollen – als Amts-, Privat- und allenfalls Geschäftsperson – fliessen alle auf den digitalen Helfern zusammen, sind jedoch sehr unterschiedlich. Wenn Amtspersonen für Politik, Geschäfts- und Privatleben ein und dasselbe Gerät verwenden, stellt dies ein Sicherheitsrisiko dar. Eine mögliche Trennung der Daten von Privat- und Amtsperson und damit eine Erhöhung der Sicherheit kann durch den Einsatz von Virtualisierungstechnologien sichergestellt werden.

Auf Basis der Virtualisierungstechnologie wird ein Zonenmodell vorgestellt, in welchem (sensitive) Informationen aus der Rolle als Amtsperson von Informationen aus der privaten / geschäftlichen Rolle abgegrenzt werden können. Wie ein solcher Lösungsansatz aussehen kann, wird im nachfolgenden Whitepaper vorgestellt.

Die unterschiedlichen Rollen einer Amtsperson

In der Schweiz hat das Milizsystem eine lange Tradition: So wird eine Vielzahl von politischen Ämtern auf Gemeindeebene bis hin zum Parlament als Milizfunktion ausgeübt. Als Vorteil einer solchen Doppelfunktion wird oft die Nähe des Parlaments zum Bürger und zur Wirtschaft im praxisbezogenen Denken und Handeln genannt. Wissen aus dem beruflichen Alltag wird in die politischen Aufgaben eingebracht. Auf der anderen Seite können diese verschiedenen Rollen als Privat-, Geschäfts- und Amtsperson zu Konflikten führen. Dies infolge der vielfältigen und teils komplexen Informationsräume, in denen sich heutige Amtspersonen bewegen. Eine saubere Trennung der oben genannten Rollen im Alltag ist dadurch fast unmöglich, was sich ebenfalls in unserem IT-Umfeld manifestiert.

Ein professioneller Umgang mit und eine starke Präsenz in den Social Media ist heute eine Voraussetzung für eine erfolgreiche Wahl und zudem aus dem politischen Alltag nicht mehr wegzudenken. Andererseits ist spätestens nach der Diskussion über die politische Einflussnahme auf Wahlen in Deutschland, Österreich und Frankreich klar, dass Amtspersonen zur Zielscheibe werden.

Für die politische Arbeit ist eine gute Vernetzung in Partei, Parlament und Wirtschaft essentiell. Zunehmend komplexere politische Dossiers werden in parteiübergreifenden Kommissionen erarbeitet. Dabei ermöglicht die Digitalisierung einen schnellen, permanenten, ortsunabhängigen und umfassenden Zugang zu benötigten Informationen. So können sich Politikerinnen und Politiker von unterwegs aus in ein Dossier vertiefen und sich auf die Kommissionssitzung vorbereiten. Dabei wird oft das Smartphone oder der Laptop als unersetzlicher digitaler Helfer eingesetzt, der auch für private und / oder berufliche Zwecke benutzt wird. Dies führt zu einer Vermischung der Daten auf einem einzigen Endgerät. So sind auf demselben Gerät Informationen zu privaten und geschäftlichen Kontakten, Parteiprogramme und Dossiers gespeichert.

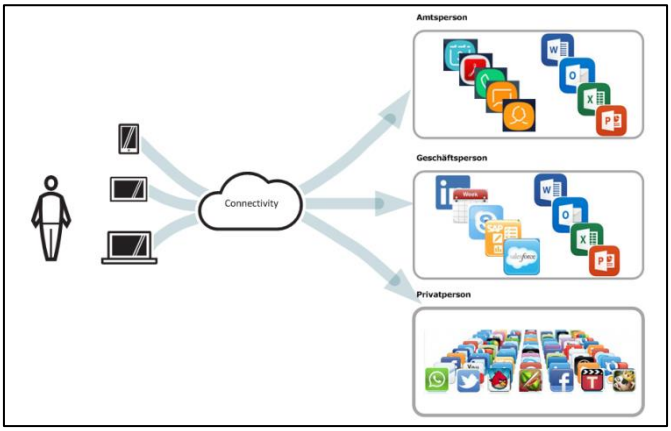


Abbildung 1: Divergierende App-Landschaften der verschiedenen Rollen

Unterschiedliche Sicherheitsanforderungen zum Schutz der Informationen

Die Schutzanforderungen für private, geschäftliche und amtsbezogene Informationen sind sehr unterschiedlich. Während die Amtspersonen für ihre privaten Informationen selbst verantwortlich sind, sind für die Sicherheit geschäftlicher und amtsbezogener Informationen die jeweiligen Organisationen zuständig. Diese erlassen ihre Informationsschutzverordnung und definieren entsprechende Schutzmassnahmen. Verwendet eine Amtsperson ihr Endgerät für ihre Rollen als Privat-, Geschäfts- und Amtsperson, führt das unweigerlich zum Sicherheitskonflikt. Wenn das Endgerät der Amtsperson auch für die Informationsbeschaffung im Internet oder für geschäftliche Aktivitäten benutzt wird, kann nicht sichergestellt werden, dass dieses Endgerät nicht durch Attacken aus dem Cyber Space betroffen ist. Parlamentarier, welche zum Beispiel einer sicherheitspolitischen Kommission oder

einer Geschäftsprüfungskommission angehören, kommen durch ihre Funktion und durch die damit verbundene Aufgabe in Kontakt mit sensitiven Dossiers. Aus diesem Grund muss sichergestellt werden, dass sensitive Informationen in einer sicheren Umgebung bearbeitet und gespeichert werden.

Zonierung durch Virtualisierung

Um all diesen verschiedenen Rollen von Amtspersonen und den Sicherheitsanforderungen der Organisationen gerecht zu werden, bedarf es einer sicheren Lösung. Die Forderung des BSI (Bundesamt für Sicherheit in der Informationstechnik) Grundschutz M4.449 Zonenkonzept und ISO 27001 A11.6.2: «Sensible Systeme müssen sich in einer dezidierten (isolierten) Umgebung befinden» bedeutet, dass die sensiblen Informationen einer Organisation nur in einer isolierten Zone bearbeitet und gespeichert werden dürfen. Diese Forderung trifft in gleichem Masse für geschäftliche, amtsbezogene und im Grunde genommen auch für private Informationen zu. Somit wird klar, dass ein Endgerät, auf dem Informationen aus verschiedenen Zonen (Internet, Privates, Geschäft, Amtsorganisation) bearbeitet werden, diese Zonen konsequent voneinander trennen muss.

Ein einzelnes Endgerät, auf dem sensible Informationen verschiedener Organisationen bearbeitet werden und das sogar noch mit den IT-Infrastrukturen dieser Organisationen in Verbindung steht, genügt somit den heutigen Sicherheitsstandards bei weitem nicht mehr.

Die Virtualisierungstechnologie stellt im Bereich IT-Sicherheit eine interessante Möglichkeit zur Zonentrennung auf einem einzigen Endgerät zur Verfügung. Durch eine Virtualisierungs-Software können auf einem Computer sogenannte Virtuelle Maschinen (VM) definiert werden, wobei sich jede dieser VMs wie ein vollwertiger Computer verhält. Alle VMs teilen sich dabei die Hardware. Innerhalb der VM werden ein Standard-Betriebssystem und die gewohnten Applikationen installiert. Der Benutzer wird dabei nicht eingeschränkt und kann mittels Mausklick zwischen diesen Betriebsumgebungen hin- und herschalten. Mittels Virtualisierung lassen sich somit mehrere unabhängige Betriebsumgebungen auf nur einer Computer Hardware parallel betreiben.

Dabei ist das Konzept der Virtualisierung schon seit 1960 von IBM verwendet worden, um einen Mehrbenutzerbetrieb zu ermöglichen. Im Rahmen der Server-Virtualisierung wird die Anzahl der Hardware reduziert und über gemeinsam genutzte Hardware werden die IT-Amortisationskosten verringert. Die virtuellen Server bieten zudem den Vorteil, dass die virtuellen Maschinen einfach verschoben und zur Laufzeit situativ mit entsprechenden Ressourcen ausgestattet werden können. Die Verwaltung erfolgt zentral per Software und kann den laufenden Betriebsbedürfnissen angepasst werden. Auf aktuell erhältlichen Hardwaresystemen können mehrere hundert virtuelle Server gleichzeitig laufen.

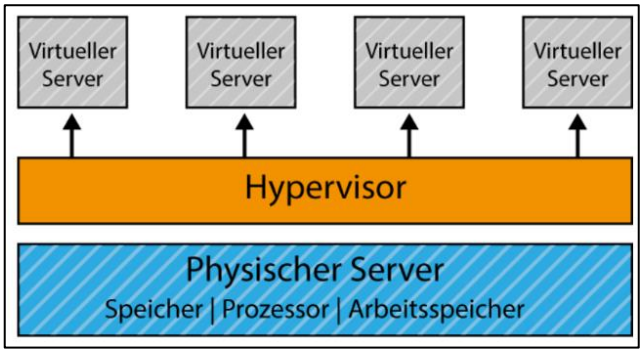


Abbildung 2: Grundprinzip der Virtualisierungstechnologie
Quelle: https://www.datenschutzbeauftragter-info.de/was-ist-ein-virtueller-server/

Damit wäre die Zonentrennung auf einem Endgerät eigentlich Realität. Doch reicht die Qualität der Zonentrennung kommerzieller Software-Produkte? Diese Frage lässt sich nicht generell mit ja oder nein beantworten. Es kommt auf die Sensitivität der Informationen an, welche in der Zone bearbeitet und gespeichert werden. Je sensibler die Informationen, umso interessanter werden diese für Cyber-Kriminelle und umso besser müssen die Informationen geschützt werden. Das Schutzniveau muss in einer Risikoanalyse ermittelt werden. Falls ein hoher Schutz erforderlich ist, reicht eine Standard-Virtualisierungs-Software nicht mehr aus.

Die VDI-Technologie

Den Schutz sensibler Informationen kann man noch zusätzlich mit dem Einsatz von «Virtual Desktop Infrastructure (VDI)»-Technologie erhöhen. Dabei wird das Endgerät lediglich noch für die Eingabe (Maus und Tastatur) und Ausgabe (Bildschirm) verwendet. Der Betrieb von Betriebssystem und Applikationen sowie die gesamte Datenhaltung werden in der zentralen IT-Infrastruktur der Organisation betrieben. Damit wird verhindert, dass Informationen lokal auf dem Endgerät gespeichert, auf ein USB-Memory Device ausgegeben oder ausgedruckt werden können.

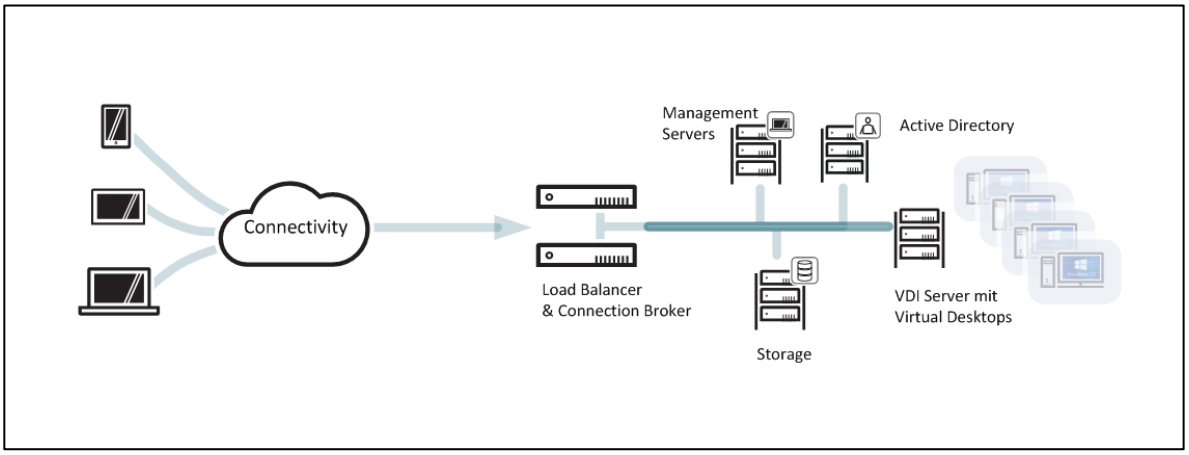


Abbildung 3: VDI-Technologie
Quelle: https://blogs.vmware.com

Die VDI-Technologie setzt dabei eine permanent verfügbare Verbindung vom Arbeitsplatz zur zentralen Infrastruktur voraus. Durch die Zentralisierung des gesamten Betriebssystems kann ein Grossteil der Wartungsaufgaben der IT zentral erledigt werden. Änderungen und Migrationen müssen so nicht mehr auf jedem Arbeitsplatz gepflegt werden. Die Verantwortung für das Endgerät kann komplett an den Benutzer abgegeben werden, so weit, dass der Benutzer sein eigenes Gerät als Zugangspunkt zur VDI-Infrastruktur verwendet. Ein Einrichten und Installieren der Software entfällt grösstenteils. Individuelle Arbeitsplätze werden dem Benutzer zugewiesen oder können durch den Benutzer per Templates gewählt werden. Gerade bei Organisationen mit häufig wechselnden Mitgliedern ist die vereinfachte Bereitstellung der IT-Umgebung über Templates ein gewichtiger Vorteil.

So setzten beispielsweise Schulen auf die VDI-Lösung, damit Lehrer und Schüler effizient die IT-Infrastruktur und benötigte Programme aus dem Schulalltag nutzen können. Bei ortsfesten Arbeitsplätzen werden «Thin Client»-Arbeitsplätze eingesetzt, welche mit einer reduzierten Hardware auskommen. Mit dem Trend des «Bring Your Own Device» (BYOD) können Schüler und Mitarbeiter mit eigenen IT-Mitteln auf die Infrastruktur der Schule zugreifen, ohne dass der Support sich um das Endgerät kümmern muss. Dies verringert IT-Support und Wartungsaufwand. Ein solches VDI-Konzept hat bereits 2013 die Friedrich-List-Schule in Berlin erfolgreich umgesetzt und ist mittlerweile ebenfalls verbreitet an Schweizer Schulen anzutreffen.

Dass der VDI-Ansatz auch für Behörden anwendbar ist, zeigt ein Beispiel einer grösseren Umstellung aus den kantonalen Behörden des Kantons Aargau. Die Abteilung Informatik Aargau stellt eine flexible Lösung auf Basis VDI für ca. 500 Mitarbeitende der Verwaltung zur Verfügung. So können Arbeitsplätze effizient verwaltet und bis auf mobile Geräte zur Verfügung gestellt werden. In der Umsetzung wurde zusammen mit einem lokalen Partner eine Citrix-Lösung umgesetzt. Dabei sind die Erfahrungen in Bezug auf Flexibilität, Benutzerkomfort und Performance erfüllt worden.

VMI-Technologie für Smartphones

Nicht mehr aus dem Alltag wegzudenken sind heute Tablets und Smartphones. Im Bereich der mobilen Endgeräte ist die Menge der Geräte und deren Ressourcen exponentiell gewachsen. Datenkapazitäten auf Memory RAM und mobilen Datenträgern wie µSD-Karten und die Prozessorleistungen erreichen Leistungen analog zu den Arbeitsrechnern im Büro. Entsprechend sind die Angriffsvektoren auf mobile Geräte besonders beliebt, da das Endgerät Zugangspunkte zu allen Bereichen unseres Lebens liefert. So ist in den letzten Jahren das Smartphone zur Benutzerinterface für ein gesamtes Ökosystem geworden. Beispielsweise öffnen wir die Eingangstüre per Smartphone, kommunizieren per App mit dem Auto, nutzen den Informationskanal zu den Social Media, bezahlen an der Kasse per TWINT und verwalten E-Mails und Kontakte von privaten und Geschäftsbeziehungen.

Das Bewusstsein, dass diese Geräte exponiert sind und aktuelle Malware vermehrt auf jene Gerätetypen zielt, ist in den letzten Jahren gestiegen. Sicherheitskonzepte wie «Multi Device Management»-Systeme (MDM) für Smartphones und «Endpoint Detection and Response (EDR)»-Lösungen für portable Geräte sind in den letzten Jahren in den Fokus gerückt.

Analog zum Trend der Virtualisierung durch VDI sind «Virtual Mobile Infrastructure (VMI)»-Lösungen für die Smartphone-Betriebssysteme (Apple, Android und Windows Mobile) erhältlich. Mit diesen lassen sich sogenannte VMI Clients, also Tablets, Smartphones und weitere portable Geräte, virtualisieren. Die Betriebssysteme und die Applikationen (Apps) laufen nicht direkt auf dem Endgerät, sondern zentral auf dem VMI-Server.

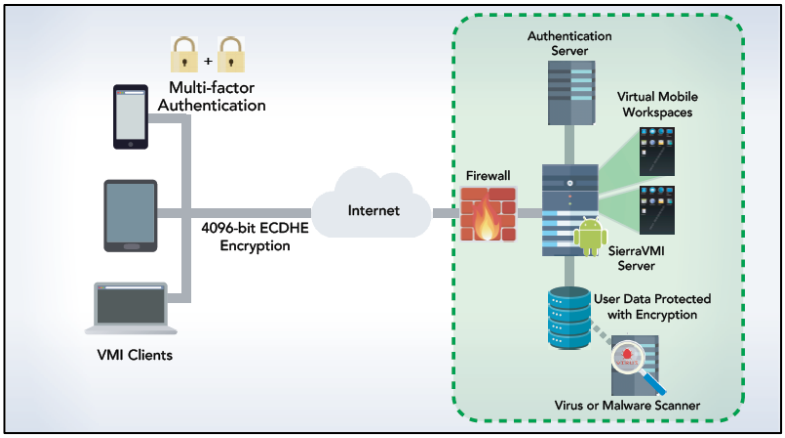


Abbildung 4: VMI-Technologie für Smartphones
Quelle: www.sierraware.com

Gerade bei mobilen Geräten ist ein Verlust des Geräts durch Diebstahl oder schlicht durch Unaufmerksamkeit häufig. So hat gemäss einer Umfrage von ESET Lost and Found bereits jeder Fünfte einmal ein Gerät als verloren oder gestohlen gemeldet. In 63 % der Fälle blieben diese Geräte unauffindbar. Werden dabei die Informationen konsequent zentral und virtualisiert gehalten, bedeutet ein Verlust des Geräts lediglich den Verlust des Zugangspunkts. Die Informationen selbst sind nicht

exponiert und der Zugang kann jederzeit durch den Support gesperrt und auf einem neuen Gerät ausgestellt werden. Auch ein Wechsel des Endgeräts erfolgt ohne Datenverlust.

CyOne SmartProtect Technology – die Kombination aus Virtualisierung und Sicherheit

Der SmartProtect Technology-Ansatz der CyOne Security liegt in der Virtualisierung von digitalen Räumen, die den Umgang mit den verschiedenen Rollen wie Amts-, Geschäfts- und Privatperson sicherstellen. Dabei stellen die privaten Geräte wie Smartphone, Tablet und Laptop die Zugangspunkte zu den verschiedenen Umgebungen dar.

Durch die Virtualisierung werden Zonen geschaffen, in denen die Privatperson alle möglichen Anwendungen nutzen kann und parallel dazu als Amtsperson klar definierbare Funktionen in sicherer Umgebung verwendet. So bleiben die Informationen gemäss den Rollen separiert, jedoch für den Benutzer auf seinem Endgerät zugreifbar.

Entsprechende sensitive Dokumente werden in geschützten und falls erforderlich klassifizierten Zonen zur Verfügung gestellt, ohne dass dabei die private Umgebung durch unnötige Einschränkungen und Vorgaben des Arbeitgebers behindert wird. Auf der anderen Seite gefährden private Facebook- und Mailkonten keine Daten aus dem politischen Arbeitsumfeld.

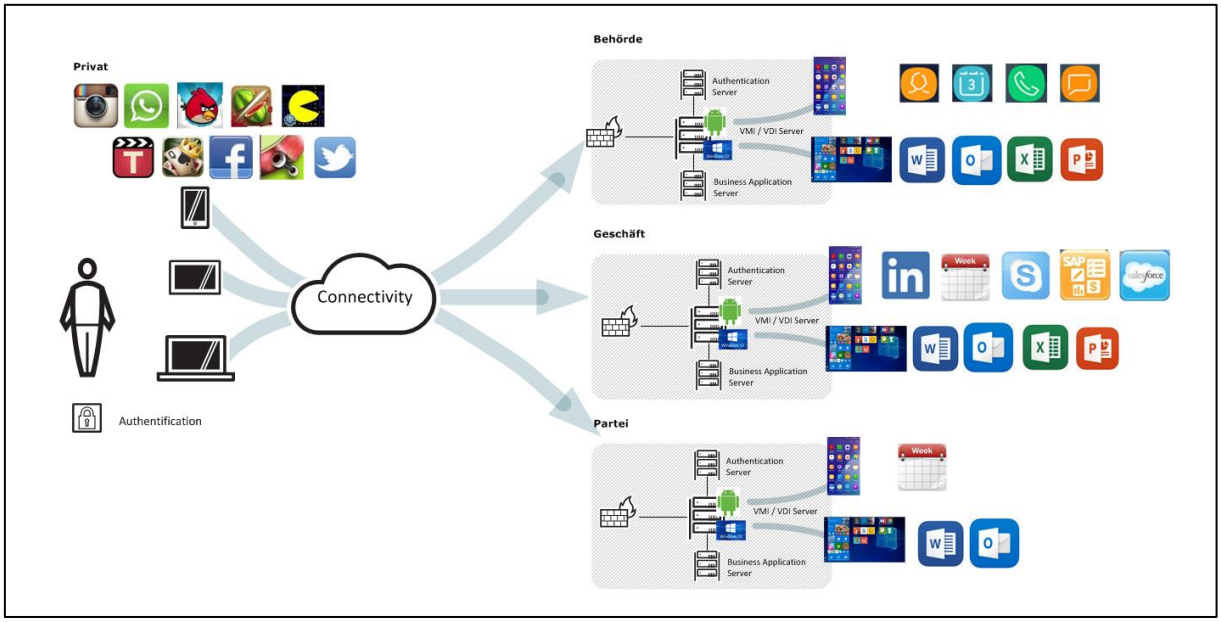


Abbildung 5: Virtualisierungsansatz der CyOne Security

Dabei liefert die VDI- und VMI-Infrastruktur die Grundlage für die gesicherten Zonen. Damit die Daten und Applikationen betrieben werden können, sind noch weitere Aspekte zu beachten. So muss eine Authentifizierung der Person vom Endgerät aus möglich sein. Dabei weisen sich Benutzer mit Credentials (z. B einer PKI-Karte) gegenüber der Plattform und den Anwendungen aus. Der Zugang zu Daten und Apps erfolgt erst nach erfolgreicher Authentifizierung.

Erweiterte Hardware wie z. B. ein PKI-Kartenleser stellt gerade auf einer mobilen Plattform eine besondere Herausforderung dar. Aus diesem Grund haben sich Alternativen wie mTAN per SMS, photoTAN oder QR-TAN als Authentifizierung auf mobilen Geräten etabliert. Als Zugangspunkt zum Virtualisierungsserver kommen mehrheitlich Gateways zum Einsatz. Diese stellen den Zugangspunkt zur Serverlandschaft (connection broker) dar und sichern den Netzwerkverkehr zwischen Endgerät und Server.

Falls es die Klassifikation der Informationen erfordert, kann für den Zugang zu bestimmten Infrastrukturen ein gehärtetes Endgerät der CyOne Security verwendet werden. Dabei wird eine dezidiert gehärtete Hardware eingesetzt. Als «Connection Broker» kommt ein Sicherheitsgateway mit Hardware-Security-Modul zum Einsatz. Somit ist neben dem Endgerät auch der Zugang zur Serverinfrastruktur gegenüber Cyber-Angriffen geschützt.

Auf dem Endgerät stellt das CyOne Security-Sicherheitsbetriebssystem volle Kontrolle über alle Schnittstellen zur Umwelt und eine oder mehrere virtuelle Umgebungen zur Verfügung. Neben dem Zugang zu klassifizierten Zonen kann durchgängig vom sicheren Endgerät aus auch auf weitere VDI-Infrastruktur zugegriffen werden. Auf diese Weise skaliert die Lösung für verschiedene Klassifikationen und es kann trotzdem einheitlich gearbeitet werden.

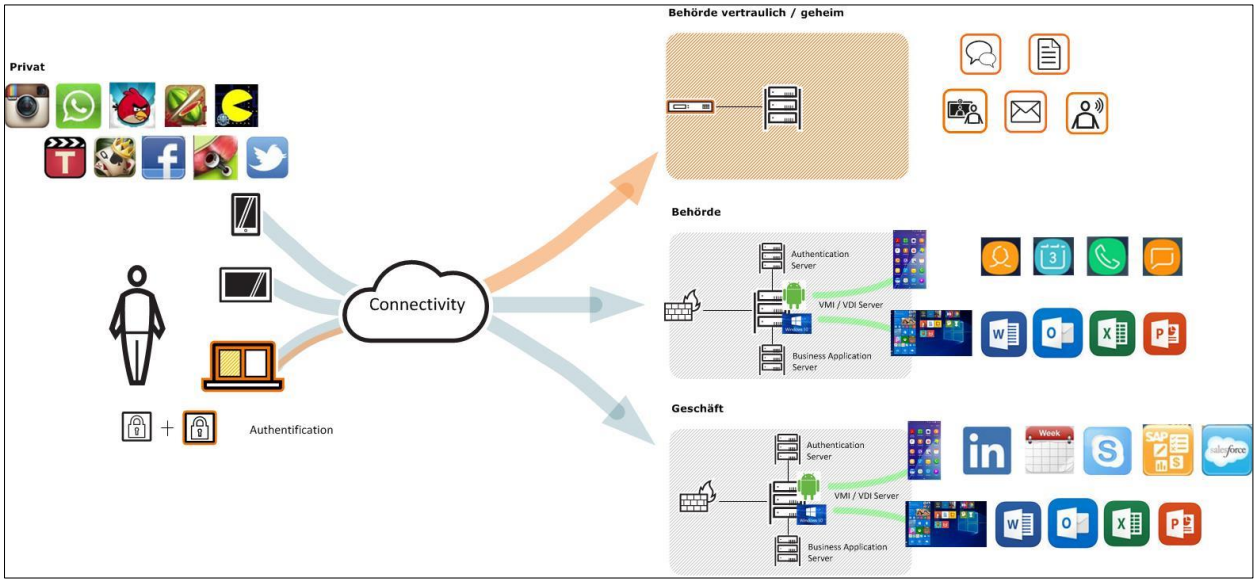


Abbildung 6: Die gehärteten Virtualisierungskomponenten der CyOne Security

Mehrwert für Amtspersonen durch «Virtuelle Informationsräume»

Der Mehrwert des CyOne Security-Lösungsansatzes für die Herausforderungen von Amtspersonen liegt in der Schaffung von «Virtuellen Informationsräumen», welche mobil zur Verfügung stehen. Die Kombination von Virtualisierung für virtuelle, digitale Räume und der skalierbaren Sicherheit ermöglicht ein durchgängiges und mobiles Arbeiten:

- Für den Benutzer ergibt sich eine Reduktion der Endgeräte. Separierte Hardware für diverse Organisationen entfallen.
- Eine Vielzahl von Endgeräten, Modellen und Ausprägungen kann über den Standardzugang vereinheitlicht werden. Dabei reduziert sich der Aufwand für die Supportorganisation auf den jeweiligen Zugang.
- Aufgrund einer breiten Kompatibilität der VDI-Lösungen kann eine Vielzahl von unterschiedlichen Endgeräten unterstützt werden. Ein «Bring Your own Device (BYOD)»-Ansatz ist dank der Technologie möglich.
- Wo gefordert, wird punktuell gehärtete Sicherheitshardware eingesetzt. Damit skaliert die Lösung über die unterschiedlichen Sicherheitsanforderungen der Informationsräume.
- Änderungen und Mutationen können zentral durchgeführt werden. Durch Bereitstellung von Templates und vordefinierten Umgebungen verringert sich der Supportaufwand.

- Verlorene Endgeräte bedeuten lediglich den Verlust des Zugangs. Die Daten sind zentral sicher abgelegt. Zugänge können einfach gesperrt und Endgeräte ohne Datenverlust migriert werden.

Aus Sicht der IT-Sicherheit bietet die VDI-Technologie den Vorteil, dass sensitive Daten zentralisiert gehalten und auf dem Endgerät lediglich während der Bearbeitung angezeigt werden. Ebenso werden keine Informationen lokal gespeichert. Dies verhindert einerseits Datenverlust im Fall eines defekten Endgeräts, andererseits aber auch einen Datenabfluss, sollte das Endgerät verloren gehen oder gar gestohlen werden. Durch die Separierung der Betriebssysteme können Dokumente, Daten und Applikationen strikt voneinander getrennt werden, und Einschränkungen durch Policies und Vorgaben der Klassifikation greifen jeweils nur in entsprechenden Bereichen.

Die Notwendigkeit einer permanenten Verbindung für VDI- / VMI-Technologie stellt für hochmobile Anwendungen (sprich fahrend unterwegs) noch eine Herausforderung dar. Dabei sind weniger die heute verfügbaren Datenbandbreiten kritisch als stabile Antwortzeiten des Netzwerks. Sobald Antwortzeiten zwischen Server und Arbeitsplatz von über 100 ms ausfallen, ist eine produktive Arbeit nicht mehr gegeben. Für mobiles Arbeiten an einem stationären Ort in der Schweiz wie im Open Space, Home Office oder am Arbeitsplatz erfüllen die heutigen Lösungen die Benutzererwartungen. Leistungseinbussen in der Performance von 5 bis 10 % werden durch leistungsstarke Hardware kompensiert und wirken sich bei durchschnittlicher Nutzung nicht spürbar auf den Betrieb aus.

Grafikbeschleunigte und rechenintensive Anwendungen können jedoch zu Limitationen führen, die dann nicht zufriedenstellend in einer virtuellen Umgebung realisiert werden können. Sobald spezifische Hardware wie z. B. Dongles oder spezielle Hardwareanbindungen auf tiefen Systemebenen benötigt werden, ist eine vertiefte Analyse zur Detailumsetzung zu empfehlen, um die Kompatibilität sicherzustellen.

Mit dem Ausbau der Netze und Mobilfunknetze sinkt der Nachteil der Latenzzeit im Mobilnetz. Waren es bei der 3G-Technologie noch 100 ms liegen die Werte im 4G-Netz noch im Bereich von 30 ms und mit der Einführung des 5G-Standards sollen diese Verzögerungen nur noch etwa 1ms betragen. Trotzdem ist heute ein hochmobiles Arbeiten z. B. im Zug oder Flugzeug noch nicht gegeben. Ebenfalls ist die Virtualisierungstechnologie nicht kostenlos und «en passant» in der Organisation verfügbar. Zwischen einer Virtualisierung im Serverbereich und dem Betrieb einer VDI- / VMI-Infrastruktur bestehen wesentliche Unterschiede. So kommen Wissen zu WAN-Optimierungen, QoS (Quality of Services) und einige Spezialitäten im Bereich der Lizenzierung von Server und Software in Zusammenhang mit der VDI-Technologie auf den Betreiber zu.

CyOne Security ist der vertrauensvolle Partner für sichere Virtualisierung

Durch die Digitalisierung und zunehmende Vernetzung werden zwangsläufig Informationsräume geschaffen werden müssen, um Systeme überschaubar sicher zu gestalten. Dabei spielt die Virtualisierungstechnologie eine entscheidende Rolle. CyOne Security entwickelt aus diesem Grund die CyOne SmartProtect Technology weiter und stellt Wissen im Bereich sicherer Virtualisierung, Zonenarchitekturen und Gateways zur Verfügung, damit Sie Ihre Rolle als Betreiber einer sicheren IT-Infrastruktur für Amtspersonen voll und ganz wahrnehmen können.

Setzen Sie dafür auf die langjährige Erfahrung und die 360°-Sicherheitskompetenz der CyOne Security. Als rein schweizerisches Unternehmen bieten wir den kundenspezifischen Risiken angepasste, umfassende Sicherheitskonzepte und -lösungen auf höchstem Niveau für Product Security, System Security sowie Operational Security an.

Beginnen Sie heute, Amtspersonen zu schützen, damit das Milizsystem nicht zum Sicherheitsrisiko wird.

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

Kontaktieren Sie uns für ein kostenloses Expertengespräch.