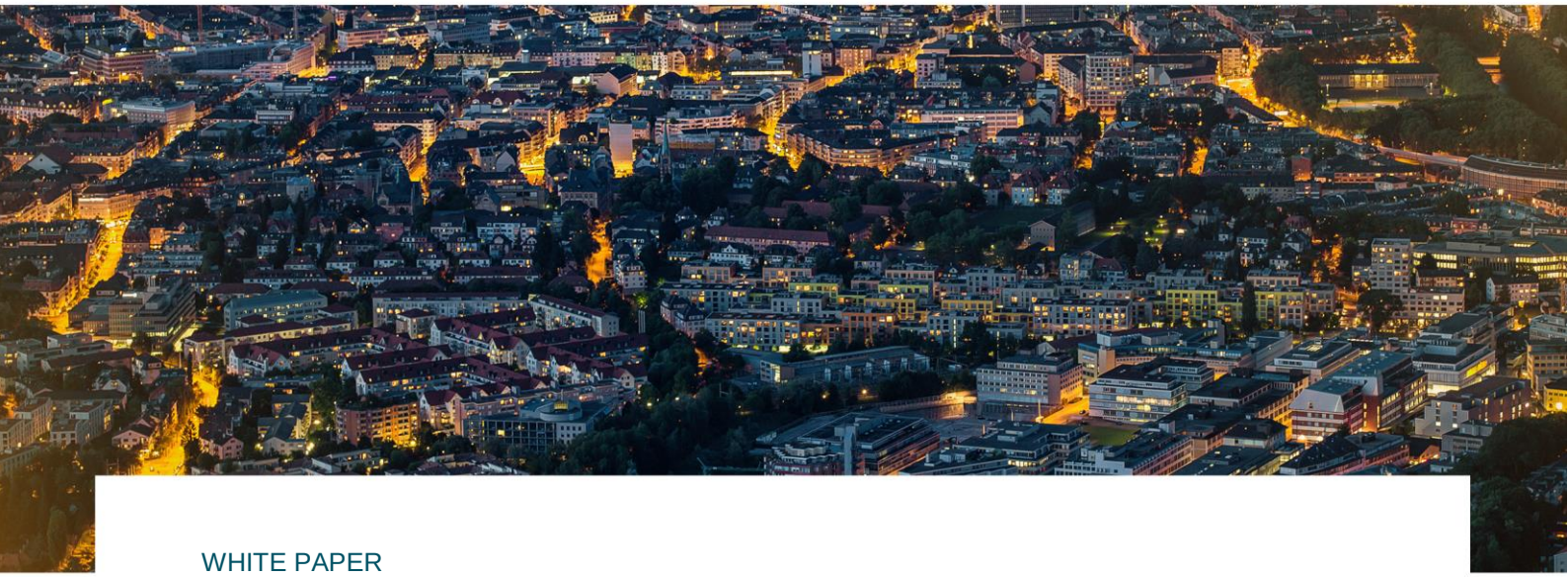
CyOne Security AG
Hinterbergstrasse 18
6312 Steinhausen

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



WHITE PAPER

Fachapplikation als sicheres Inselsystem

Reto Amstad | Senior Security Consultant | Steinhausen, 19. Februar 2019

Die Harmonisierung und Standardisierung von IT-Arbeitsplätzen stellt für die Bearbeitung von sensitiven Daten eine Herausforderung dar. Als mögliche Lösungen werden die Daten entweder konsequent in allenfalls gehärteten dezidierten Systemen bearbeitet. Alternativ wird versucht, die Daten auf den Standardsystemen mit zusätzlichen Sicherheitsmechanismen zu schützen. Besser ist es aber, das gesamte System hochsicher gekapselt einzubetten.

Sobald UCC als Sprach- und Kollaborationsplattform in eine existierende und standardisierte Büroautomatisationsumgebung integriert wird, wächst deren Komplexität. Für den verantwortlichen CISO stellt die notwendige Risikoanalyse und Sicherheitsbeurteilung dann eine äusserst komplexe Herausforderung dar. Als möglicher Lösungsweg bietet sich an, die sensitiven Daten in entsprechenden Fachapplikationen zu verarbeiten und diese auf dezidierte Systeme auszulagern.

Gemäss den (Sicherheits-)Anforderungen wird in diesen Fachapplikationen ein reduzierter Funktionsumfang festgelegt und dank klaren Systemgrenzen und Datenhaltungskonzepten durch die eigene Organisation betrieben. Somit ist der Weg frei, die Standard-IT-Lösung zusammen mit Partnern oder «As a Service» zu beziehen. In diesem White Paper erfahren Sie, wie neue oder bestehende Fachapplikationen in einem gehärteten IT-System mit hohem Schutzbedarf sicher gekapselt werden können – ganz ohne Benutzereinschränkungen, in gewohnter Arbeitsumgebung und ohne höhere Betriebs- und Wartungsaufwände für den Betreiber.

Trend bei den Behörden zum Infrastruktur-Outsourcing

Durch eine hohe Standardisierung von IT-Umgebungen, können grosse Einheiten von Behörden in Gemeinden, Kantonen und beim Bund mit gleichen oder zumindest ähnlichen IT-Systemlandschaften arbeiten. Diese Harmonisierung minimiert Schnittstellen und fördert die Arbeitseffizienz. Für den Betreiber andererseits bedeutet diese Infrastruktur-Standardisierung einen kleineren Betriebsaufwand und ein dezidierteres IT-Know-how. Beides resultiert schlussendlich in tieferen Kosten für die betroffenen Behörden. Zunehmend wird darum der IT-Betrieb teilweise oder ganz ausgelagert, entweder an Partnerbehörden oder an private Firmen. Folgende Vorteile ergeben sich daraus:

- Entlastung der IT-Abteilungen, was eine Fokussierung auf deren Kernfähigkeiten ermöglicht
- Einfacher Einbezug von Spezialisten-Know-how von aussen mit aktuellem Spezialwissen
- Skalierbare IT, welche sich rasch den wechselnden Anforderungen anpasst
- Transparenz durch klare Kosten für Aufwände in Projekten und Change Management
- Verlagerung des Fachkräftemangels und höhere Spezialisierung der Fachkräfte beim Partner

Gefahren dieses Trends in Bezug auf die Daten

Die Praxis zeigt, dass die vorhandenen IT-Strukturen und ihre Anwenderlandschaften hoch komplex sind und weitreichende Abhängigkeiten aufweisen (siehe Abbildung 1).

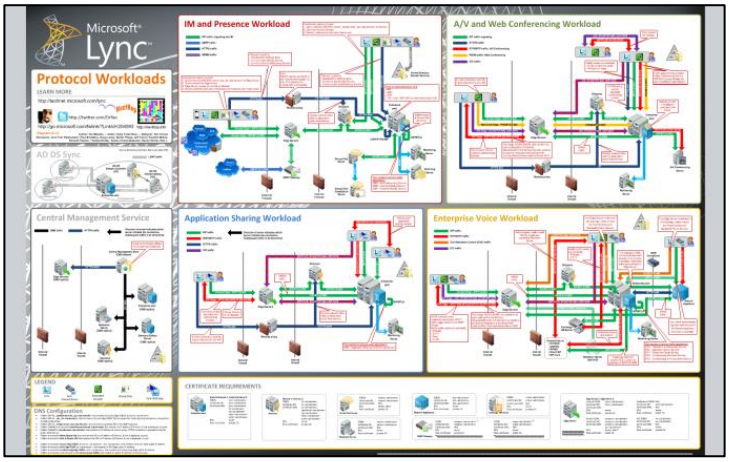


Abbildung 1: Microsoft Lync Server 2010 Communications Software Protocol Workload Poster
Quelle: mslync2010.worldpress.com

Die Auswirkungen und die Abhängigkeiten in Bezug auf Sicherheit können dadurch oftmals nicht abschliessend beurteilt werden. Innerhalb dieses Outsourcing-Prozesses muss zudem der Umgang mit den klassifizierten Daten gelöst werden. Dies stellt sowohl die betroffenen Behörden als auch die Betreiber vor grosse Herausforderungen.

Mit dem Outsourcing von IT-Kompetenzen stellt sich für die betroffene Behörde immer die Frage, wie weit ein detailliertes System- und Architekturverständnis intern bewahrt werden kann bzw. beibehalten werden soll. Immerhin geht es hier um die Fähigkeit der Sicherheits-Awareness und das grundlegende Verständnis für hochsichere ICT-Plattformen. Andererseits wird dieses teure IT-Spezialwissen lediglich bei Architekturänderungen benötigt. Für die betroffene Organisation stellt sich damit die Frage der Wirtschaftlichkeit dieser Spezialisten.

Bei einer Auslagerung der IT liegen unter Umständen die sensiblen Daten selber und / oder sogar die Zugriffe auf die entsprechenden Systeme und damit auf die sensiblen Daten beim gewählten Partner. Der Zugriff und der Umgang mit diesen Daten müssen daher klar geregelt sein. Dabei steht fest, dass die Verantwortung für die Daten immer bei der Organisation selbst verbleibt. Schadenereignisse wie Systemausfälle durch Stromunterbruch, Wasser, Feuer etc. können und müssen schriftlich abgesichert werden. Allfällig entstehende Schäden durch Datenverlust oder ungewollten Datenabfluss können jedoch nur bedingt juristisch per Service Level Agreement (SLA) an den Partner weitergegeben werden. Schwer messbar sind eventuelle Reputationsschäden für die betroffene Behörde und den involvierten IT-Partner aufgrund eines Ereignisses.

Aus Sicht der Cyber-Sicherheit bietet die Auslagerung potenziell eine höhere Angriffsfläche. Schliesslich erstreckt sich das Netzwerk bis zum Partner. Somit muss der Partner zwingend in die Sicherheitsbetrachtung einbezogen werden. Dieser steht dadurch vor der Herausforderung, dass sein Core-Netz, aber auch sein Kundennetzwerk genügend stark segmentiert sein müssen, damit unter seinen betreuten Mandanten keine Schadsoftware «wandern» kann, oder der vermeintliche Partner eine Schwachstelle im ICT-Konzept darstellt. Das Nachverfolgen, wer wann wo auf Kundendaten zugegriffen hat, bedingt hohe Audit-Anforderungen und eine höchst strukturierte Arbeitsmethodik des Partners. Oftmals sieht ein Alltag des ICT-Supports heute so aus, dass schnellstmöglich alles wieder zum Laufen gebracht wird. Dabei verwenden mehrere Administratoren die gleichen Accounts und Passwörter, dies sogar für mehrere Mandanten. IT-Systeme und Server werden per Script aufgesetzt und oft wird dabei vergessen, die Standard Passwörter abzulösen. Aus Sicht der IT-Sicherheit ist damit die notwendige Nachvollziehbarkeit als Grundprinzip nicht gegeben.

Herausforderungen bei dezidierten gehärteten Systemen mit Fachapplikationen

Es ist fahrlässig zu glauben, selber kein potenzielles Ziel von Cyber-Attacken zu sein. Aktuelle Vorfälle aus dem Cyberspace zeigen, dass immer öfter gezielt Mitarbeitende als Angriffsziel ausgesucht (target attacks) und als potenzielle Einstiegsportale in die IT-Infrastruktur einer Organisation benutzt werden. Dazu setzen die Angreifer massgeschneiderte Malware ein, um in einem ersten Schritt Zugang zu privilegierten Benutzerprofilen zu erhalten, in einem zweiten Schritt unbemerkt Infrastrukturpläne, Geheimdienstinformationen, Strategiekonzepte, Befehle oder vertrauliche Protokolle stehlen, modifizieren, chiffrieren oder löschen zu können.

Ein möglicher Lösungsansatz für die komplexe und vernetzte IT bietet die Auslagerung der sensitiven Daten in entsprechende Fachapplikationen auf dezidierte Systeme. Dabei werden die Systeme vereinfacht und sind dadurch auch aus Sicht der IT-Sicherheit überschaubarer. Sensible Daten können aber nicht nur klassifizierte «intellectual property» sein. Auch Personendaten wie Lohnregister, Steuerdaten, polizeiliche Fahndungs- und Falldaten oder biometrische Artefakte sind für Behörden und Unternehmen schützenswerte Informationen.

Die nachfolgende Abbildung zeigt eine klassische Referenzarchitektur mit einer dezidierten Fachapplikation (siehe Abbildung 2).

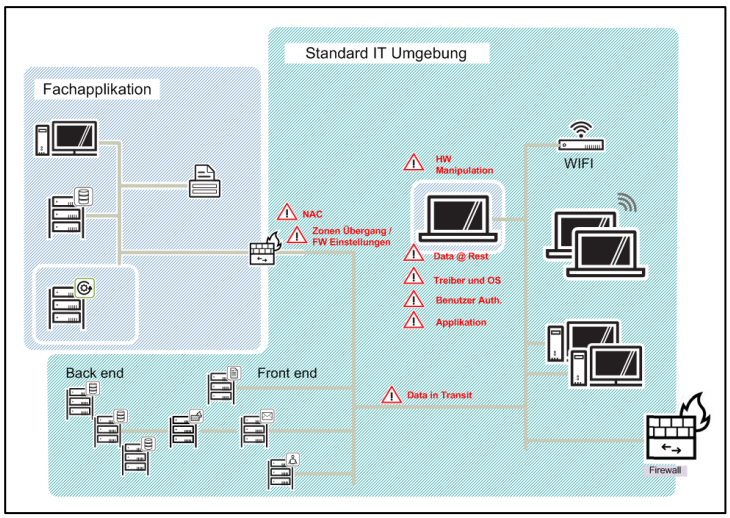


Abbildung 2: Referenzarchitektur einer Insellösung

Muss eine Behörde klassifizierte Berichte sicher bearbeiten und ablegen können, wird infolge der hohen Sicherheitsanforderungen oft ein zusätzliches System zur Verfügung gestellt (siehe Bereich Fachapplikation). Dort werden die Daten erstellt, bearbeitet und abgespeichert. Zwingend ist zudem eine starke restriktive Benutzerauthentifizierung auf dem dezidierten System, sollen doch nur berechtigte Personen Zugang zu diesen Daten haben.

Weiter müssen Daten «at rest» auch bei ausgeschaltetem System gesichert abgelegt werden und dadurch vor Diebstahl oder Entwendung gesichert sein. Falls eine zentrale Ablage oder zentrale Dienste gewünscht sind, muss der Rechner mit der entsprechenden Fachapplikation mit einer zentralen Infrastruktur abgleichen. Die Daten können offline per USB oder über das Netzwerk gesendet werden. Durch die zentrale Infrastruktur können mehrere Personen gemeinsam mit derselben Datenbasis arbeiten, und es lassen sich Back-ups, protokolliertes Exportieren etc. realisieren.

Was sind die Sicherheitsherausforderungen?

Digitale Information ist nicht direkt an den Träger gebunden. Dies erkennt man spätestens dann, wenn die Daten eingeschlossen werden sollen. Was für Information auf Papier und für den Prozess der Bearbeitung von klassifizierten Dokumenten gut etabliert ist, kann für digitale Daten nur bedingt angewendet werden. So kann nur der Datenträger, das Notebook oder der Server im Tresor eingeschlossen werden. Sobald Daten elektronisch bearbeitet werden, sind diese automatisch an mehreren Orten vorhanden wie z. B. im Speicher, auf der Disk und auf dem Bildschirm. Falls diese sogenannten digitalen Artefakte unerlaubt kopiert oder eingesehen werden, ist dies, wenn überhaupt, nur auf entsprechenden System-internen Protokollen sichtbar.

Ansätze, digitale Daten vor unerlaubtem Zugriff zu sichern, bieten kryptografische Funktionen. So ist es heute «Best Practice», Hard Disks, Datenbanken und Files zu chiffrieren. Die richtige Implementierung der Chiffrierung ist dabei grundlegend. Kann verifiziert werden, dass die Chiffrierung richtig im vorhandenen System eingesetzt wird und kann verifiziert werden, dass die Chiffriertechnologie richtig angewendet wird? Wichtige Fragen sind hier zum Beispiel: Wo sind Zugangsdaten (in Form von Schlüsseln, Zertifikaten, PINs und Passwörtern) abgelegt? Sind sie im

Betrieb ohne Einschränkungen verfügbar und trotzdem sicher verwahrt? Kommt die geforderte Chiffrierung tatsächlich zur Anwendung? Wie gut ist die Software vor Manipulation geschützt? Die Spanne von möglichen Chiffriermitteln reicht dabei von Freeware Tools für den Heimgebrauch über Bordmittel eines Betriebssystems bis hin zur perfomanten Realtime-Harddisk oder Datenbank-Chiffrierung. Eine gemeinsame Herausforderung haben alle. Wie kann eine korrekte Implementierung der Sicherheit verifiziert werden? Die Vergangenheit hat gezeigt, dass in den heutigen Applikationen wie z.B. Office-gängige Betriebssysteme wie Windows, die Treibersoftware, aus einigen Millionen Zeilen Code besteht, welche letztlich auf dem Benutzerrechner laufen. Somit verwundert es nicht, wenn im Code immer wieder Bugs entdeckt werden, welche einen Cyber-Angriff (Exploit) erlauben. Eine vollständige Überprüfbarkeit von Softwareimplementierungen (OS, Driver, Fach-applikationen) ist heute für ein Unternehmen daher fast unmöglich.

Herausforderungen bei Kapselung

Beim klassischen Härten wird von einem Standard-System ausgegangen, welches dann durch Analyse und Behebung von Schwachstellen gesichert wird. Im Betriebssystem und den installierten Software-Paketen werden nicht benötigte Prozesse und Funktionalität deaktiviert bzw., wenn möglich, entfernt. Hier stellt sich in der Praxis die Herausforderung, dass Software-Teile stark ineinandergreifen und voneinander abhängig sind. So können Treiber und Teile des Betriebs-systems nicht ohne weiteres deaktiviert werden, ohne Auswirkungen auf weitere Funktionen des Betriebssystems zu haben. Ein Deaktivieren eines Treibers schaltet zwar dessen Funktionalität aus. Dies heisst aber nicht, dass er nicht wieder aktiviert werden kann. Ein vollständiges Entfernen des Codes ist oftmals nur mit sehr hohem Aufwand möglich, da Code-Teile und Treiber mehrfach verwendet werden. Deshalb werden gehärtete Systeme selten aktualisiert.

Netzwerktechnisch werden über sogenannte Zonierungen spezifische Geräte in Subnetze separiert. «Network Access Control (NAC)»-Lösungen isolieren die Geräte aufgrund von Eigenschaften oder Zertifikaten. Dabei liegt das Vertrauen bezüglich der Sicherheitsqualität dieser Separierung einerseits beim Hersteller der NAC-Lösung und andererseits in einem hohen Mass auch beim IT-Betreiber, welcher die NAC-Lösung konfiguriert. Spezifische Systeme können auch in komplett separater Netzwerk-Hardware umgesetzt werden. Der benötigte Aufwand für die Betreuung einer solchen Parallelinfrastruktur ist aber enorm. Zudem leidet die Flexibilität.

Ein konträrer Lösungsansatz bietet die Virtualisierung. Hier wird die potenziell unsichere Umgebung per Host-Betriebssystem von der Hardware getrennt. Das Host-Betriebssystem definiert die Schnitt-stellen zur Hardware und kann so eine Standard-Umgebung kapseln. Das Betriebssystem (z.B. Linux, Windows 10) und die Anwendungen (z.B. Office) der Anwendungsumgebung laufen virtuell und sind vom Host-Betriebssystem des Benutzerrechners durch den Host gekapselt.

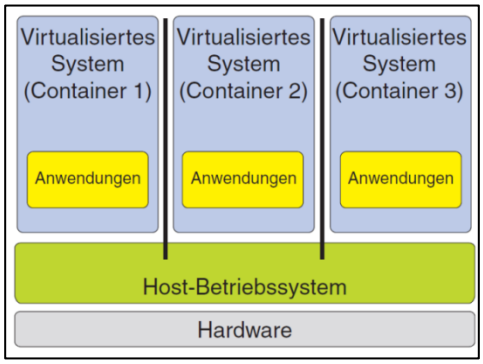


Abbildung 3: Virtualisiertes Betriebssystem
Quelle: Christian Baun, Karlsruher Institut für Technologie, Steinbuch Centre for Computing (SCC)

CyOne Security – Lösungsansatz zur Kapselung

Basierend auf dem Ansatz der Virtualisierung wurde die CyOne SmartProtect Technology realisiert. Dabei wurde das Host-Betriebssystem als Sicherheitsbetriebssystem CyOne SmartProtect OS entwickelt. Das Sicherheitsbetriebssystem stellt Sicherheitsfunktionen für den Benutzer und für die Hardware zur Verfügung und kontrolliert sämtliche Schnittstellen. Somit kann eine Standard-Umgebung vollständig gekapselt werden. Ein Betriebssystem inklusive dessen Anwendungen (z.B. Sharepoint) der Anwendungsumgebung laufen virtuell und sind vom Sicherheitsbetriebssystem des Benutzerrechners mit Hilfe der CyOne SmartProtect Technology sicher umhüllt.

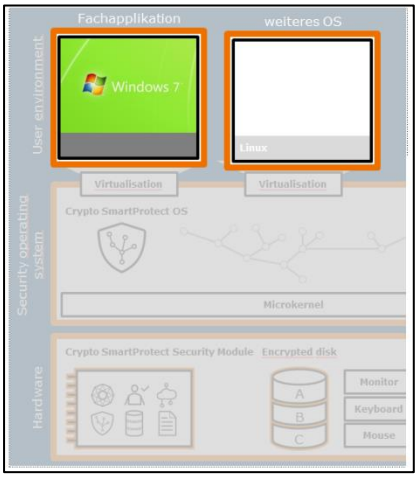


Abbildung 4: Lösungsansatz zur Kapselung der CyOne Security AG

Sämtliche In- und Output-Schnittstellen werden kontrolliert und per Sicherheitsbetriebssystem definiert. Daten können nur auf den definierten Verbindungen via sicheren IP-VPN-Kanal zur zentralen Infrastruktur ausgetauscht werden. Die Betriebssysteme und Anwendungen der Arbeits-umgebung(en) sind chiffriert abgelegt und somit gegen Modifikationen geschützt. Zusammen mit dem Schutz vor Manipulation der Hardware und einer starken Zweifaktorauthentifizierung ist der Benutzerrechner bestens gegen Angriffsvektoren geschützt, dank dem sicheren Inselsystem mit CyOne SmartProtect Technology. Die Gesamtlösung eines sicheren Inselsystems besteht aus dem Benutzerrechner mit der Fachapplikation und allenfalls einer zentralen Infrastruktur inklusive Management-Komponenten.

Um ein geschlossenes und sicheres System zu garantieren, werden die Daten auf einem geschützten Benutzerrechner bearbeitet. Aus Sicherheitsgründen dürfen die Dokumente selber das System bei der Erstellung und Bearbeitung nicht verlassen. Dazu kann ein klassifizierter Notebook eingesetzt werden, welches die starke Benutzerauthentifizierung und mittels der Harddisk-Chiffrierung den Schutz «at rest» garantiert. Falls eine Verbindung zur zentralen Infrastruktur benötigt wird, ist diese kryptografisch geschützt und komplett per VPN logisch getrennt. Deshalb kann als Transportnetzwerk ein bestehendes IT-Netzwerk oder gar das öffentliche Netz (Internet) genutzt werden – mit dem Vorteil einer hohen Mobilität der Lösung. Dabei müssen keine aufwän-digen parallelen Netzwerkinfrastrukturen erstellt und betrieben werden.

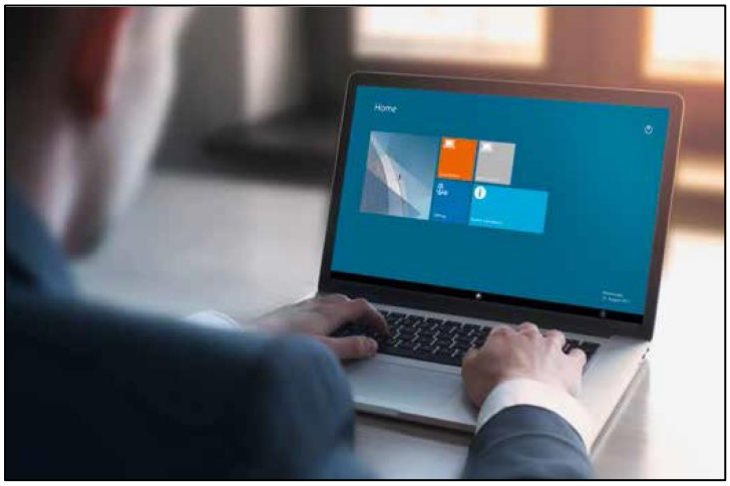


Abbildung 5: Arbeiten mit einem Benutzerrechner

Die Benutzerrechner bestehen aus Notebooks mit der CyOne SmartProtect Technology. Ein Compartment entspricht dabei der Arbeitsumgebung inklusive der Fachapplikation. Dabei können auch bestehende Betriebssystemumgebungen und Fachapplikationen migriert werden. Das Betriebssystem CyOne SmartProtect OS stellt zusammen mit dem Hardware-Sicherheitsmodul die sicheren Verbindungen über zur Verfügung stehende Netzwerke in die zentrale Infrastruktur her. Alle Schutzmechanismen laufen unbemerkt im Hintergrund, ohne den Arbeitsprozess zu beeinträchtigen. Die Benutzerrechner können an stationären Standorten per Docking Station oder mobil betrieben werden.

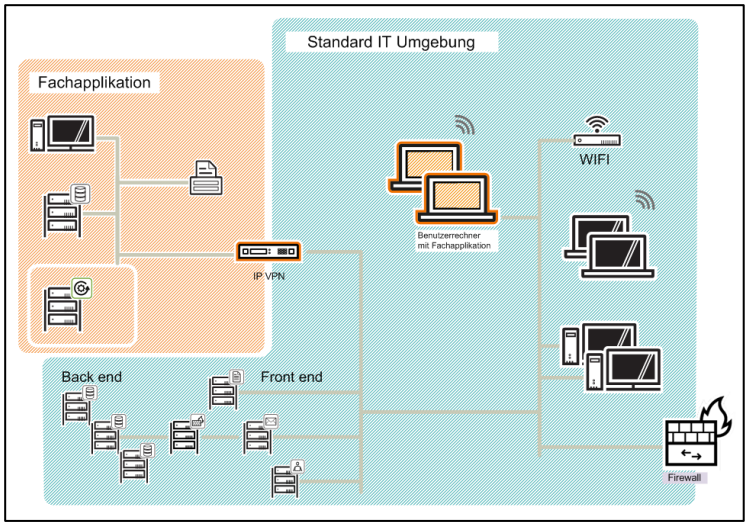


Abbildung 6: Fachapplikation als Inselsystem innerhalb der Standard-IT

Die zentrale Infrastruktur stellt dabei die notwendigen Funktionen zur Verfügung. Dies können Datenbanken, Dokumentablage und Back-up-Prozesse sein. Falls notwendig, können an der zentralen Infrastruktur definierte Sicherheitsschleusen realisiert werden, so dass Nutzdaten und Dokumente protokolliert und kontrolliert ausgedruckt oder an weitere Systeme verteilt werden können. Ebenfalls zentral wird die IT-Administration realisiert, allenfalls mit entsprechenden Schnittstellen zur Standard-IT für Systemmeldungen zwecks Überwachung des Systems. Ein allfälliges Einbringen (Kopieren) von Daten in die Infrastruktur und eventuell das Exportieren etwaiger Daten / Erzeugnisse, z.B. als Ausdruck, wird lediglich zentral protokolliert umgesetzt.

Dank der hardwarebasierten VPN-Verbindung zwischen dem Benutzerrechner und der zentralen Infrastruktur wird sichergestellt, dass aus dem Transportnetzwerk Angriffsvektoren absolut minimal gehalten werden. Somit können bei Bedarf Zugriffe direkt aus der öffentlichen Infrastruktur wie dem Internet verwendet werden, um von einem mobilen Benutzerrechner auf die Fachapplikation zuzugreifen, ohne dass dabei eine Exposition der Daten stattfindet.

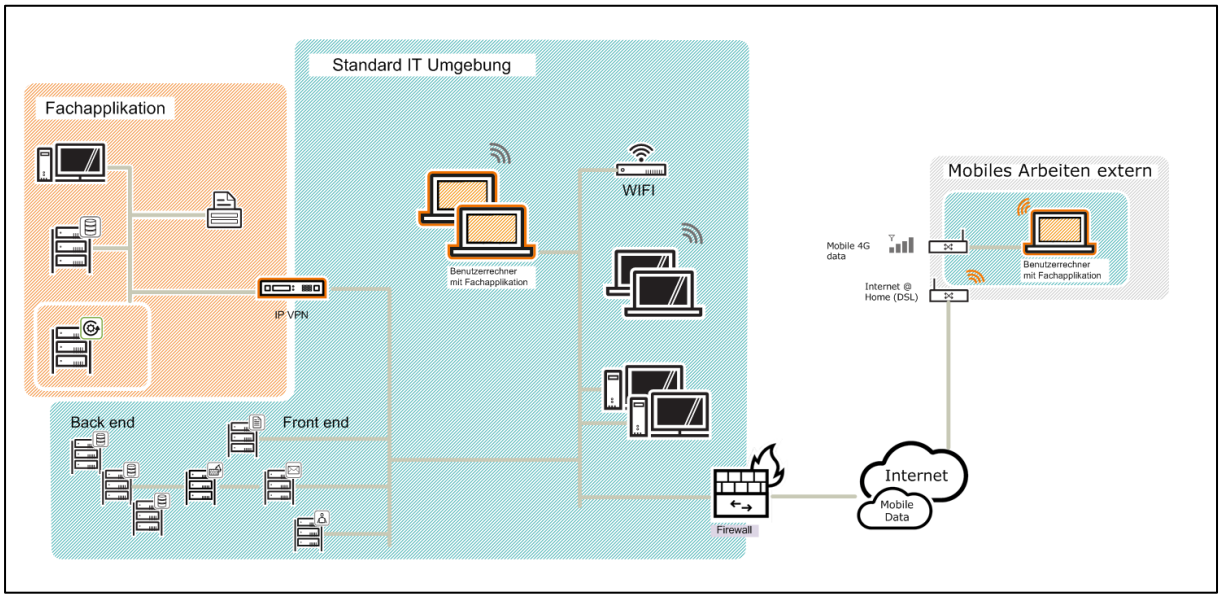


Abbildung 7: Remote-Zugriff auf die Fachapplikation über öffentliche Netze

Sicherheitsbetrachtungen

Basierend auf einem Hardware-Sicherheitsmodul bietet die CyOne SmartProtect Technology Schutz gegen Cyber-Angriffe.

Abbildung 8: CyOne SmartProtect Security Module und Encrypted Disk

Authentifizierung

Das System verfügt über eine starke 2-Faktor-Authentifizierung. Die Benutzer-Smartcard stellt einen Faktor dar (Besitz). Weiter wird ein Passwort verlangt als Zugang zum Benutzerrechner (Wissen). Innerhalb des virtuellen Betriebssystems können die gewohnten Benutzer-Log-ins eingerichtet werden z. B. über eine Standard-Log-in-(Microsoft)-Authentifizierung.

Emergency Clear

Der Benutzer kann am Benutzerrechner einen sogenannten Emergency Clear auslösen. Damit werden die Kommunikationsschlüssel und der Zugang zur Harddisk gelöscht und es ist kein Zugang zu den Arbeitsumgebungen und zur zentralen Infrastruktur mehr möglich. Der Zugang kann natürlich über das Zentrale Management wieder freigegeben werden.

Secure Boot
Das Sicherheitsbetriebssystem wird während des Starts überprüft und ist gegen Manipulation geschützt. Die Software und das Host-Betriebssystem werden geschützt gespeichert und können nicht manipuliert werden.

Updatefähigkeit des Host-Betriebssystems
Updates des Sicherheitsbetriebssystems können zentral sicher verteilt werden, sodass jederzeit definierter Softwarecode auf dem Benutzerrechner läuft.

Encrypted Storage
Eine transparente Harddisk-Chiffrierung erfolgt im Hintergrund und schützt die Daten – auch bei ausgeschaltetem Benutzerrechner.

Sicherer Netzwerkzugang
Ein hardwarebasiertes VPN-Netzwerk ermöglicht eine saubere Zonentrennung auf dem Transportnetzwerk und garantiert, dass nur dezidierte Benutzerrechner mit CyOne SmartProtect Technology auf die zentrale Infrastruktur zugreifen dürfen.

Die Architektur der Software folgt dem Grundsatz Security by Design und bietet bei Cyber-Attacken eine kleinstmögliche und kontrollierte Angriffsfläche.

Betriebskonzept und notwendige zentrale Managementfähigkeiten

Durch die Kapselung können die Betriebssystemumgebung und die Fachapplikation / Applikationen wie gewohnt durch den Administrator verwaltet werden. Die zentrale Infrastruktur kann dadurch z.B. über WSUS-Aktualisierungen an Windows sicherstellen, dass die neusten Patches eingespielt sind oder dass die Fachapplikation automatisch auf den neusten Stand aktualisiert wird. Somit kann ein gewichtiger Nachteil des Härtens – nämlich, dass Systeme nach jedem Update überprüft und verifiziert werden müssen oder sich gar nicht mehr updaten lassen – elegant umgangen werden.

Das Management der Benutzerumgebung und der Fachapplikation kann innerhalb der sicheren Zone erfolgen. Für das Sicherheitsbetriebssystem und die Netzzugänge steht eine Management Appliance zur Verfügung. Auf einem Server werden die benötigten virtuellen Maschinen für das Management der CyOne SmartProtect-Komponenten installiert. Darauf werden die Zugangsschlüssel und die Benutzer verwaltet. Über einen Firmware Update Server werden neue Releases bereitgestellt.

Die zentrale Infrastruktur kann in einer physisch geschützten Umgebung installiert werden. Die Bereitstellung der Umgebung mit Rack, Stromversorgung und IT-Netz und Zugang aus dem öffentlichen Netz, kann somit einem Partner abgegeben werden. Der Betrieb der Insellösung reduziert sich somit auf die wesentlichen Kernfunktionen.

Vorteile des sicheren Inselsystems

- Klare und sichere Separierung der Daten und eine sichere Datenhaltung in verifizierbaren IT-Umgebungen. Dies erlaubt neue und moderne Zusammenarbeitsmodelle mit Outsourcing-Partnern für die Standard-Büroumgebung
- Gewährleistung der Datenhoheit beim Datenurheber mit klar regelbaren Zugriffs-berechtigungen
- Bestehende Netzwerkinfrastrukturen können als Transportnetzwerk verwendet werden – der Aufbau und der Betrieb von dezidierten Lösungen entfallen dadurch komplett
- Keine Eigenentwicklung oder Sonderlösung; Standard-Tools für den Benutzer und IT-Referenzen können angewandt werden
- Die Host-Umgebungen können durchgängig sicherheitsverifiziert werden, von der eingesetzten Virtualisierungs-Umgebung bis hin zum sicheren und geschützten Netzwerkzugang
- Updatefähigkeit des Sicherheitsbetriebssystems und des Anwenderbetriebssystems inklusive Fachapplikation sind zentral mit Standard-Tools möglich
- Volle Kontrolle der erlaubten Hardware Interfaces über das sichere Host-Betriebssystem

CyOne Security ist der vertrauensvolle Partner

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, Ihre Organisation und somit die Schweiz vor Cyber-Risiken zu schützen.

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.