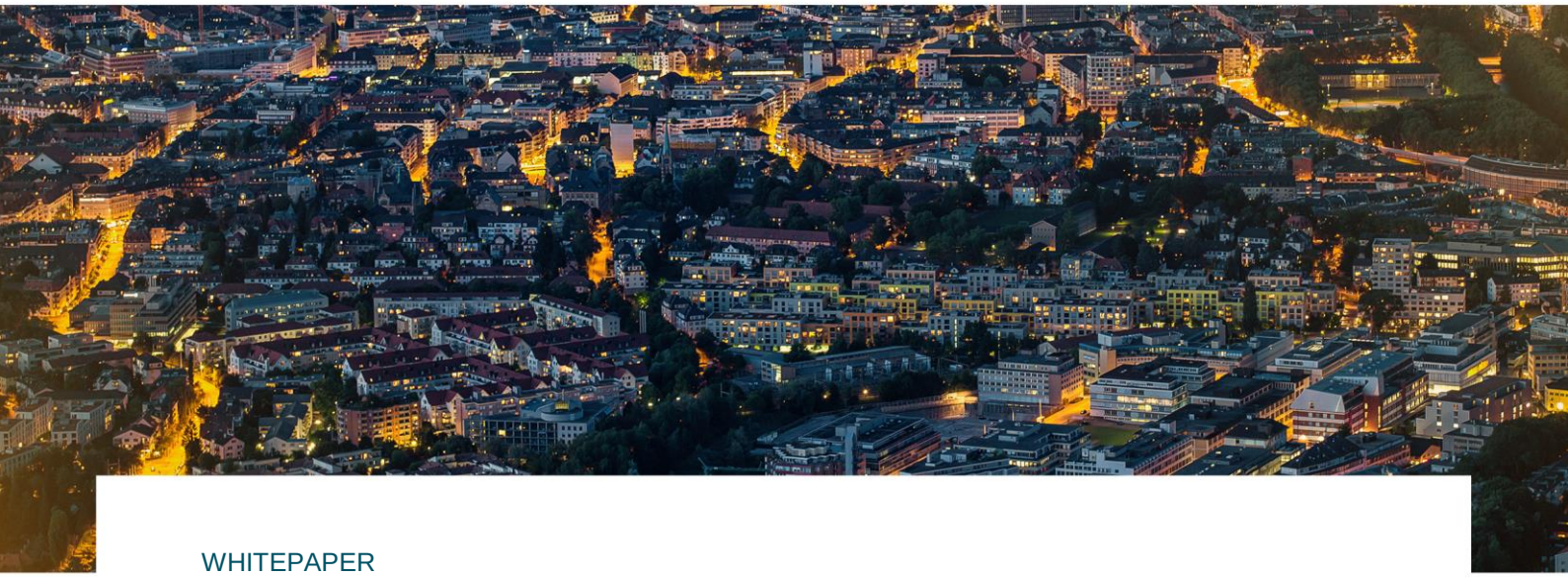
CyOne Security AG
Hinterbergstrasse 18
6312 Steinhausen

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



WHITEPAPER

Vernetzte Schliessanlage – cyber-resistent und skalierbar für jeden Schutzbedarf

CyOne Security | Steinhausen, 09. August 2022

Vernetzte Schliessanlagen weisen gegenüber den rein mechanischen Schliessungen eine Unmenge von Vorteilen auf. So können beispielsweise verlorene Zutrittsmedien deaktiviert werden, ohne das entsprechende Schloss wechseln zu müssen. Alle Zutritte können durch Log-Dateien auditiert und die Verwaltung der Zutritte kann zentral geplant und durchgeführt werden, auch wenn das Unternehmen weltweit über Niederlassungen verfügt.

Natürlich bergen vernetzte Schliesssysteme neben allen operationellen und wirtschaftlichen Vorteilen auch Gefahren. Grundsätzlich vergrössert eine unüberlegte Vernetzung die Angriffsfläche für unerlaubten physischen Zutritt oder insbesondere auch für gezielte Cyber-Angriffe.

In diesem Whitepaper wird der CyOne Security-Lösungsansatz vorgestellt, welcher – abgestimmt auf die Gefährdung des Unternehmens (Industrie, Banken- / Versicherungssektor und Behördenumfeld) – für eine vernetzte Schliessanlage angeboten werden kann. Der präsentierte skalierbare Lösungsansatz umfasst dabei ein Spektrum von Standard-Sicherheits-anforderungen bis hin zu Anforderungen mit höchstem Schutzbedarf.

Was sind mechatronische Schliesssysteme?

Traditionell kennen wir aus unserem privaten Umfeld (z.B. bei einem Mehrfamilienhaus) die mechanische Schliessung. Als eine rein mechanische Schliessanlage bezeichnen wir eine Kombination aus mechanischen Schliesszylindern und dazugehörigen Schlüsseln. Sie sind im Schliesssystem aufeinander abgestimmt. Dadurch können bestimmte Schlüssel zu mehr oder weniger Türen Zugang gewähren.

Ein Schliesssystem mit elektronischen Schlüsseln ist eine Alternative zu den rein mechanischen Systemen. Es besteht aus elektronischen Komponenten, etwa dem Türschloss oder Türlesegerät und den Zutrittsmedien. Die Zutrittsmedien umfassen heutzutage Tags, Smartcards oder sogar Smartphones mit installierter entsprechender App (siehe Abbildung 1).

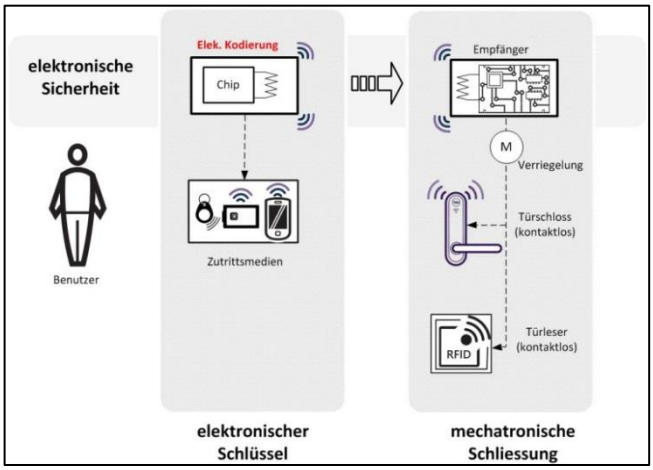


Abbildung1: Elektronische Schlüssel mit mechatronischer Schliessung

Die Identifikation der Zutrittsberechtigung wird elektronisch kodiert (z. B. mittels einer Smartphone-App) von den Zutrittsmedien (Transponder) an den Empfänger übermittelt, dies meist draht- und kontaktlos. Stimmt der Code, wird die Verriegelung der Tür über einen mechatronischen Entriegelungsvorgang freigegeben und der Zutritt ist möglich.

Ein weiterer Lösungsansatz, welcher die Sicherheit aus beiden Welten kombiniert, stellen mechatronische Schlüssel dar. Durch die Verbindung von mechanischen und elektronischen Komponenten auf dem Schlüssel des Benutzers einerseits und die Kombination einer mechatronischen Schliessung mit einem mechanischen Schliesszylinder an der Tür andererseits, wird die Sicherheit zusätzlich erhöht (siehe Abbildung 2).

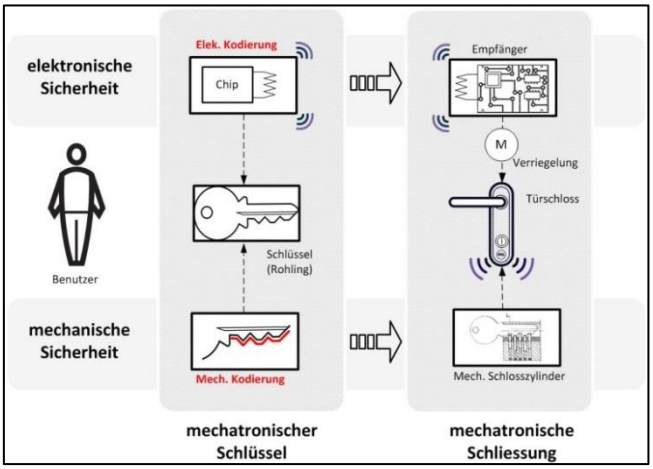


Abbildung 2: Mechatronischer Schlüssel mit mechatronischer Schliessung

Der Schlüssel besitzt damit sowohl eine mechanische Kodierung oder ein Geheimnis (z.B. Loch-tiefen, Winkel, Bohrabstände etc.) als auch eine elektronische Kodierung. Diese ist als Elektronikkomponente zusätzlich im Schlüssel eingebaut. Will der Benutzer mit seinem mechatronischen Schlüssel das Schloss öffnen, prüft dieses kontaktlos mit der vorhandenen Elektronik zuerst die elektronische Kodierung des Schlüssels. Wenn diese korrekt ist, wird der mechanische Schlosszylinder mechanisch freigegeben (Entriegelung).

In einem zweiten Schritt wird nach der Einführung des Schlüssels in den Schlosszylinder die mechanische Kodierung durch den eingebauten Türzylinder mechanisch überprüft. Erst wenn alle Zuführungen des Schlüssels passen, kann der Rotor des Zylinders gedreht und die Tür geöffnet werden. Der mechatronische Schlüssel ermöglicht in diesem Sinne eine zweifache Authentifizierung.

Um die Schlüsselmedien und die Schliessungen zentral verwalten zu können, bieten die Hersteller von solchen mechatronischen Schliesssystemen softwarebasierte Verwaltungstools an. Diese speichern die entsprechenden Schliesspläne, Authentifizierungs- und Datenchiffrierungscodes in einer Datenbank ab. Die einzelnen Schlüsselmedien können dann entweder mittels eines speziellen Programmiergeräts (offline) oder via Netzwerk (online) administriert werden.

Die Offline-Variante ist für den Betreiber mit einem hohen Betriebsaufwand verbunden. Um alle Vorteile einer mechatronischen Schliessung optimal nutzen zu können, werden meistens die Online-Variante oder Teile davon gewählt (Vollvernetzung oder Teil-Vernetzung).

Typischer Aufbau einer vernetzten Schliessanlage

Die nachfolgende Abbildung zeigt schematisch den Aufbau einer vernetzten Schliessanlage für ein Unternehmen mit mehreren geografisch getrennten Filialen (siehe Abbildung 3):

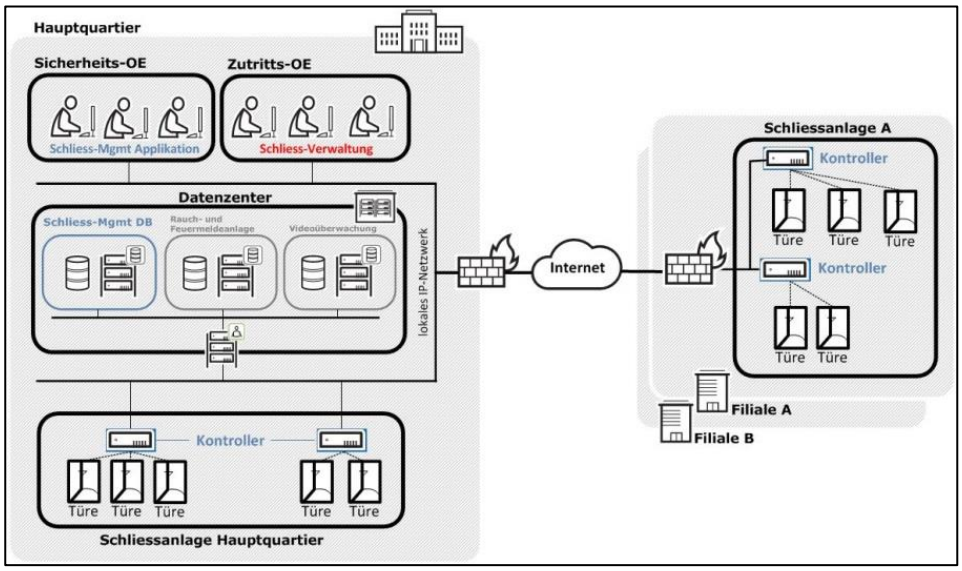


Abbildung 3: Schematische Darstellung einer vernetzten Schliessanlage

Innerhalb von Unternehmen sind zum Teil mehrere Sicherheitsorganisationen für die Fragen der Zutritte zuständig. Da gibt es zum einen eine Sicherheitsvorgabeorganisation, welche für die Zutritte und damit für den unternehmensweiten Schliessplan verantwortlich ist. Dort werden einerseits die Lesegeräte und / oder elektronischen Türen konfiguriert. Diese Konfigurationen können elektronisch über ein entsprechendes IP-Netzwerk an die internen und an die filialweiten Zugänge verteilt werden. Andererseits werden innerhalb dieser Organisation die initialen Zutrittsmedien (Tags, Badges,

mechatronische Schlüssel etc.) programmiert und an die Mitarbeitenden abgegeben. Für den operativen Betrieb ist meistens eine andere Organisation zuständig (z.B. Loge, Wachdienst etc.). Diese ist für den täglichen reibungslosen Betrieb und für eine allfällige Intervention verantwortlich. Dort können entsprechende temporäre Konfigurationen geladen werden, wenn Mitarbeitende ihren «Badge» vergessen haben oder über das Netzwerk mögliche Remote-Öffnungen durchführen (z.B. bei einer Warenanlieferung etc.).

Sämtliche Schliesskonfigurationen und Log-Daten werden in einer herstellereigenen zentralen Datenbank gespeichert. In vielen Fällen befindet sich diese Datenbank in einem Datencenter auf einem dezidierten Server. Beide Organisationen können über ein lokales Firmennetzwerk auf diesen Datenbank-Server zugreifen. Meistens laufen auf diesem Netzwerk innerhalb einer eigens dafür definierten Sicherheitszone noch weitere sicherheitsrelevante Systeme wie z.B. Videoüberwachungs-, Alarm-, Feuer- und Rauchmeldeanlagen. Die Filialen werden aus Kostengründen oft via öffentliches Netz (Internet) an den Hauptsitz angeschlossen.

Welche Vorteile haben vernetzte Schliesssysteme?

Vernetzte Schliessanlagen mit mechatronischen Komponenten – sei es nun mit elektronischen Zutrittsmedien und passenden Lesegeräten und / oder mit einem mechatronischen Schliesszylinder – weisen gegenüber rein mechanischen Schliesssystemen die folgenden Hauptvorteile auf:

- Zutrittsberechtigungen einzelner Personen können aktiviert oder deaktiviert werden (Flexibilität)
- Zutritte von Personen können ausgelesen werden (Auditierbarkeit)
- Verlorene Zutrittsmedien oder mechatronische Schlüssel können deaktiviert werden
- Es kann eine Teil- oder Vollvernetzung einer Schliessanlage vorgenommen werden
- Es können Fernöffnungen durchgeführt werden
- Verwaltung von verschiedenen Schliessanlagen von einem zentralen Punkt aus – weltweit

Welche (Cyber)-Gefahren bergen vernetzte Schliesssysteme?

Natürlich bergen vernetzte Schliesssysteme neben allen operationellen und wirtschaftlichen Vorteilen auch Gefahren. Grundsätzlich vergrössert eine unüberlegte Vernetzung die Angriffsfläche; dies gilt insbesondere auch für gezielte Cyber-Angriffe. Die nachfolgende Abbildung zeigt schematisch mögliche Angriffspunkte auf eine vernetzte Schliessanlage (siehe Abbildung 4).

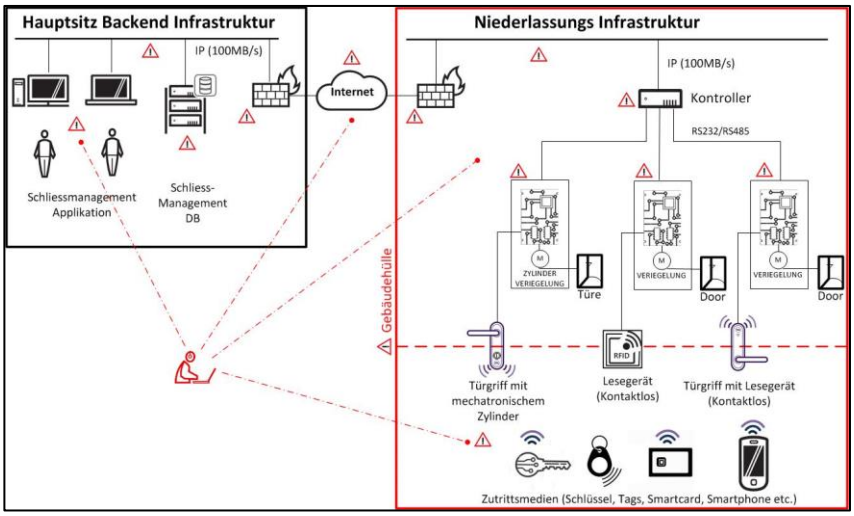


Abbildung 4: Auswahl von möglichen Cyber-Angriffspunkten bei einem vernetzten Schliesssystem

Generell lassen sich die möglichen Cyber-Angriffspunkte in vier Bereiche einteilen:

- die Netzwerkübergänge ins öffentliche Netz (sowohl am Hauptsitz als auch bei den Niederlassungen)
- die Backend-Infrastruktur mit Server-Client-Infrastruktur des herstellerspezifischen Schliessmanagements (on-premise oder Cloud-basiert)
- die Schliessinfrastruktur mit den notwendigen Kontrollern, Umsetzern und Türlesegeräten in Mietobjekten (Niederlassungen und evtl. sogar im Hauptsitz)
- die entsprechenden Zutrittsmedien, welche kontaktlos über entsprechende Luftschnittstellen entsprechende Zutritte bei den Lesegeräten anfordern können

Nachfolgend werden diese aufgelisteten Gefahrenpotenziale genauer betrachtet.

Netzwerkübergänge vom / zum öffentlichen Netz

Wie bei jedem Internetzugang ist auch im Rahmen einer vernetzten Schliessanlage dieser Übergang ein mögliches Einfallstor für Cyber-Kriminelle von aussen. Er muss daher speziell geschützt und überwacht werden. Dies sowohl auf der Seite des Hauptquartiers wie auch in den entsprechenden Niederlassungen. Es ist wichtig, dass ausschliesslich identifizierter und legitimierter IP-Verkehr das jeweilige Intranet erreicht.

Backend-Infrastruktur mit Schliessmanagement (Client-Server-Architektur)

Hier ist es möglich, dass Innentäter oder bereits eingedrungene Cyber-Kriminelle entsprechend Zugang zum zentralen Schliessmanagement-Server oder zu einem der Schliessmanagement-Clients erhalten können. Je nach Sicherheitsanforderungen bieten einzelne Hersteller bereits eine cloudbasierte Lösung an. Hat ein Angreifer aber Zugriff auf den Server – egal, wo dieser nun steht – erhält er auch sämtliche Kenntnisse über den Schliessplan. Damit kann er alle mit dem Management vernetzten Zutritte unternehmensweit (Hauptquartier und Aussenstellen) kontrollieren. Gleiches gilt auch für die Schliessmanagement-Applikation. Der Angreifer kann, wenn er die Login-Daten extrahieren oder umgehen kann, unternehmensweit Zutritte manipulieren.

Schliessinfrastruktur in Mietobjekten

Viele Unternehmen inkl. Behörden haben ihren Hauptsitz resp. ihre Niederlassungen (Filialen, Aussenstellen) in gemieteten Objekten. So ist es beispielsweise für das EDA (Eidgenössisches Departement für auswärtige Angelegenheiten) mit seinen zahlreichen Botschaften weltweit üblich, sich im Gastland an geeigneter Lage einzumieten. Dies bedeutet in beiden Fällen, dass die Aussenhülle dieser Gebäude durch den Vermieter kontrolliert werden kann. Die notwendigen Verbindungen vom öffentlichen Netzwerkzugang bis hin zum Kontroller sind damit aus cyber-technischer Sicht angreifbar. Ebenfalls problematisch sind die ganzen Zutritte der verantwortlichen Verwaltung, die Regelungen der Zutritte in ausserordentlichen Lagen (Feuerwehr) sowie die Kompatibilitätsfragen zu anderen Mietern (z.B. gleiche Haupttüre etc.).

Ein weiterer wichtiger Sicherheitsaspekt ist die mechanische Sicherheit der Kontroller und der eingebauten Türelektronik. Ist diese durch den Vermieter zugänglich, können hier entsprechende Manipulationen vorgenommen werden und so unberechtigte Personen zu einem geschützten Raum oder einem geschützten Bereich des Unternehmens Zutritt bekommen. Diese Komponenten, wenn sie nicht in einer geschützten Zone installiert werden können, sollten durch entsprechende Tamper-Massnahmen geschützt werden.

Sicherheit der kontaktlosen Zutrittsmedien

Ein wesentlicher Bestandteil der Sicherheit eines kontaktlosen Zutrittssystems ist die sichere Übertragung der Authentifizierungsdaten vom Zutrittsmedium (Transponder) zum entsprechenden Türlesegerät (Receiver). Die nachfolgende Tabelle zeigt eine Übersicht über die verschiedenen Produkte sowie deren Sicherheitseinschätzungen (siehe Abbildung 5).

Vendor	Tag	Frequency	Function	Mem (bits)	Authentication	Encryption	UID (bits)	Emulation Possible	Secure	Doc
Atmel	Temic T5557	125 kHz	r/w	330	32Bit Password Send in clear	no	40	yes	no	1
	Temic T5567									2
	Temic T5577			363						2
NXP	Hitag1	125 kHz		2048	2x32Bit Keys and 4x32 Bit Passwords	yes	32		no	3
	Hitag2			256	48Bit Key and 24 Bit Password					4
	HitagS-256					no				5
	HitagS-2048			2048						5
	Mifare Classic	13,56 MHz		8K und 32K	48Bit Key	yes	32 oder 56			13
	Mifare Desfire			32K	112Bit Key		56		no	14
	Mifare Desfire EV1			16K, 32K, 64K	56, 112, 128, 168 Bit			no	yes	
	Mifare Desfire EV2									
EM Microelectronic	EM4450	125 kHz		1024	32Bit Password Send in clear	no	32	yes	no	6
	EM4550									6
	EM4205			512						7
	EM4305									7
	EM4469						32 plus 10 Bit CustomerCode			8
	EM4200		Readonly (UID)	0	no		128		no	9
	EM4100						64			10
	EM4102									11
	TK4100									12
Legic	Prime	13,56 MHz	r/w	1-16K	no	no	32	yes	no	15
	Advant			16-64K	56, 112, 128, 168 Bit	yes	56	no	yes	

Abbildung 5: Übersicht über die kontaktlosen Zutrittsmedien und deren Sicherheit
(Quelle: Open Source Security, 2016)

Die Tabelle zeigt auf, dass entsprechende (vor allem ältere) Produkte gebrochen werden konnten. Für diesen Sicherheitsteilaspekt sind darum aus Sicht von CyOne Security nachfolgende Punkte für einen Betreiber essentiell:

- Ausschliesslicher Einsatz von starken Algorithmen für die Datensicherheit und den sicheren Datentransfer (z.B. AES)
- Die Überprüf- und Validierbarkeit der Implementierung der eingesetzten Chiffrieralgorithmen
- Richtige Implementierung und Anwendung des Chiffrierschlüsselmanagements
- Validierung der Qualität des Zufallsgenerators für die Generierung der Chiffrierschlüssel

Falls die entsprechenden Expertisen für diese Validierungspunkte beim Betreiber nicht vorhanden sind, könnte die CyOne Security hier ihr Fachwissen dem Kunden zur Verfügung stellen und gemeinsam mit ihm eine entsprechende Überprüfung durchführen.

Natürlich haben die verschiedenen Unternehmen und Behörden unterschiedliche Sicherheitsanforderungen an ein vernetztes Schliesssystem. Diese sind abhängig von der Branche, dem Tätigkeitsfeld und der Exponiertheit des entsprechenden Unternehmens.

Umso wichtiger ist es, dass entsprechende Lösungen diesem Umstand Rechnung tragen können und mittels modularer Add-ons das Sicherheitsniveau erreicht werden kann. Und zwar von Unternehmensanforderungen mit Standardsicherheit bis hin zu Anforderungen mit höchster Sicherheit für Rüstungsunternehmen und für das Behördenumfeld.

CyOne Security-Lösungsansatz für skalierbare Sicherheit

Um den unterschiedlichen Bedürfnissen von Industrie und Behörden gerecht werden zu können, wäre es sinnvoll, das vernetzte Schliesssystem bedarfsorientiert mit zusätzlichen Sicherheitsfunktionalitäten (Add-ons) ausrüsten zu können (siehe Abbildung 6).

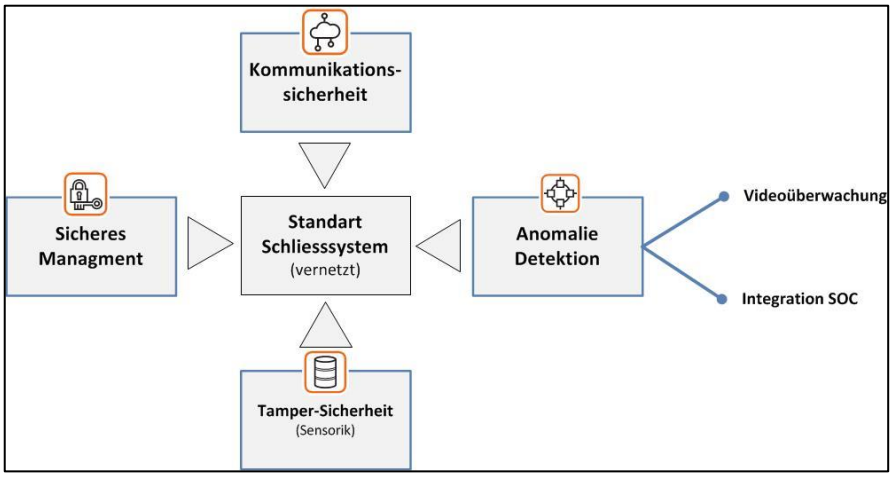


Abbildung 6: Sicherheitsmodule für Sicherheits-skalierbares vernetztes Schliesssystem

Durch diese zusätzlichen Sicherheitsmodule könnten die verschiedenen oben beschriebenen Cyber-Gefahren, spezifisch und skalierbar minimiert werden. Dabei umfassen die einzelnen Module nachfolgende Funktionalität:

Kommunikationssicherheits-Modul

Mit dem Kommunikationsmodul sollen sämtliche Verbindungen des vernetzten Schliesssystems mittels einer starken verifizierbaren Chiffrierung geschützt werden. Dies umfasst sowohl IP- als auch andere Kommunikationsverbindungen (RS-232, RS-485 über CAT5 etc.) im Bereich der Kontroller-Tür-Kommunikation. Mittels der einzigartigen Sicherheitsarchitektur der CyOne Security kann ein durchgängiger Schutz, ausgehend von den Management-Clients zur zentralen Managementdatenbank, den öffentlichen Verbindungen zu den verschiedenen Aussenstandorten bis hin zu den Kontrollern und den einzelnen Türmodulen erreicht werden. Andererseits wird mit der eingesetzten Sicherheitsarchitektur bereits eine erste strikte Zonentrennung erzielt. Damit werden mögliche Cyber-Angriffe auf den Transportwegen von und zu den verschiedenen Schliessanlagekomponenten verunmöglicht.

Für die drahtlose Kommunikation von den Zutrittsmedien zu den Türtranspondern sollen weiterhin die handelsüblichen Produkte verwendet werden können. Dadurch wird eine mögliche Interoperabilität zu allfällig anderen Mietern aufrechterhalten (z.B. infolge der Benutzung der gleichen Haupteingangstüre). Die eingesetzten kryptografischen Mittel und Prozesse könnten auf Wunsch des entsprechenden Unternehmens vorgängig durch Experten der CyOne Security einer Sicherheitsverifizierung unterzogen werden.

Sicheres Schlüsselmanagement-Modul

Das zentrale Herzstück und somit auch die Achillesferse der Sicherheit eines vernetzten Schliesssystems ist das Schlüsselmanagement. Es enthält alle relevanten Daten (Schliessplan, Authentifizierungs- und Datenchiffriercodes etc.). Es muss daher besonders geschützt werden. Dies gilt für die Schliessanlagen-Daten, welche auf einem eigenen Server im unternehmenseigenen Rechen-zentrum liegen oder ganz besonders für Daten, die bei einem Outsourcing-Partner liegen oder sogar in einer Cloud.

Durch die langjährige Erfahrung der CyOne Security im Umgang mit sensitiven Daten könnten hier mit einem möglichen Schlüsselmanagement-Modul einerseits die Daten mittels einer starken verifizierbaren Chiffrierung zugriffsgeschützt in der Datenbank gespeichert und sicher und optimal integriert über das bereits vorhandene Kommunikationsmodul verteilt werden.

Tamper-Sicherheit

Damit eine physische Manipulationssicherheit der Kontroller und der Ansprechelektronik für die Türen gewährleistet werden kann, könnten diese in tamper-resistente Gehäuse eingebaut werden. Die CyOne Security verfügt durch ihre Expertise in diesem speziellen Bereich über das notwendige Know-how.

Die internen Sensoren in diesen speziellen Gehäusen würden bei einem Sicherheitsvorfall sofort die sensitiven Daten löschen und entweder das zentrale Managementsystem in der Zentrale über den geschützten Kanal informieren oder optional über das Anomaliedetektions-Modul ein mögliches Incident Response Team (CERT) oder Security Operation Center (SOC) etc. alarmieren. Dieser Prozess könnte beispielsweise auch an ein «Cyber Defense Center (CDC) as a service» weitergeleitet werden. In beiden Fällen könnte das betroffene Unternehmen oder der damit beauftragte Partner eine Intervention einleiten.

Anomaliedetektions-Modul und Integration in Überwachungssysteme

Das Anomaliedetektions-Modul kann das vernetzte Schliesssystem in interne oder extern betriebene Cyber-Defence-Organisationen (CERT, SOC, CDC etc.) integrieren. Dabei werden einerseits entsprechende Netzwerkanomalien aus dem Schliessanlagennetz und andererseits Anomalien von den Schliess-Managementkomponenten sicher an das vorhandene Cyber-Defence-System (z.B. Splunk) übermittelt.

Zusätzlich werden aber sämtliche Tamper-Sensoren und Schliess- und Öffnungsvorgänge, welche das zentrale Management sammelt, auf entsprechende unlogische Anomalien hin überprüft (z.B. zeitliche geografische Öffnung von zwei unterschiedlichen Türen mittels gleichen Zutrittsmediums etc.). Dies mit Unterstützung von KI (Künstliche Intelligenz). Auch diese Daten werden an das Cyber-Defence-System weitergereicht und allenfalls mit Video-Überwachungsdaten angereichert.

Denkbares Sicherheitsskalierungs-Modell

Es sollte das Ziel dieses Lösungsansatzes sein, dass die oben beschriebenen Sicherheiten modular und flexibel hinzugefügt werden können. Dadurch kann aus Sicht der CyOne Security eine skalierbare Sicherheit – angepasst an die spezifischen Bedürfnisse der entsprechenden Behörden / Unternehmen erreicht werden. Eine mögliche Zusammenstellung der einzelnen Module inklusive der möglichen Branchen zeigt nachfolgende Abbildung (siehe Abbildung 7).

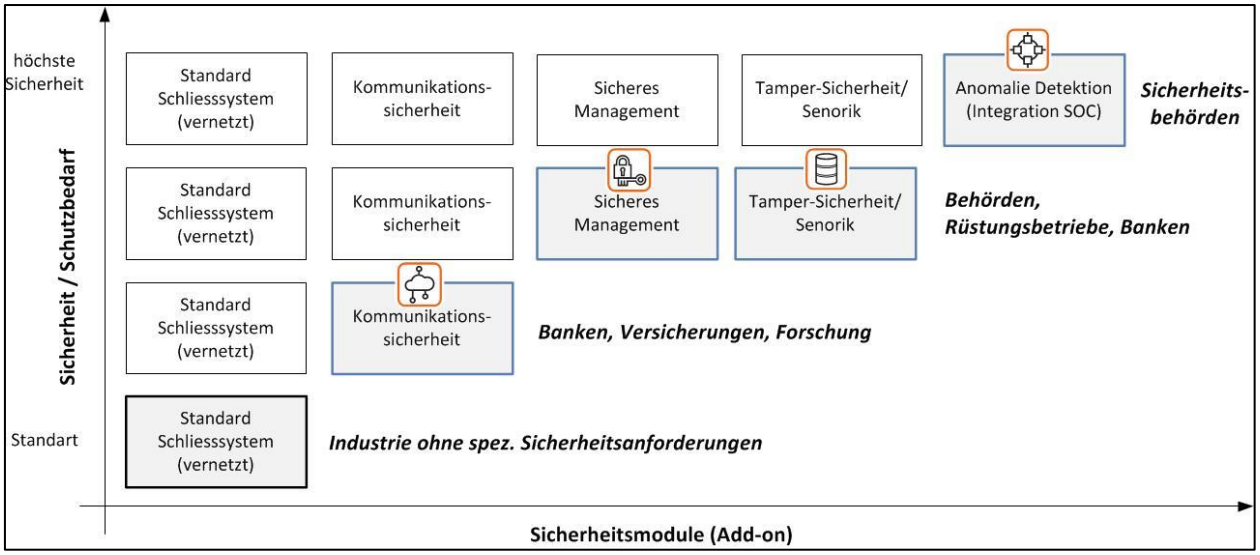


Abbildung 7: Zusammenstellung der Module für die möglichen Branchen

Die Abbildung zeigt klar auf, dass mit jedem zusätzlichen Modul höhere Sicherheitsanforderungen erfüllt werden könnten. Welche Module, für welchen Bedarf aber tatsächlich zum Einsatz kommen, wird vermutlich erst die Detailanalyse abschliessend aussagen können.

Beginnen Sie heute und schützen Sie Ihre Schliessanlagen vor Cyber-Risiken.

Machen Sie den ersten Schritt: Analysieren Sie gemeinsam mit unseren Experten die aktuellen und zukünftigen Sicherheitsbedürfnisse Ihrer vernetzten Schliessanlage, damit wir mit Ihnen über zielgerichtete Sicherheitslösungen diskutieren können.

Kontaktieren Sie uns für ein kostenloses Expertengespräch.