VIDEO® EXTRA

Vorsicht ist besser als Nachsicht

Effektive Cybersecurity schützt auch Videosicherheitstechnik vor Missbrauch

Seite 3

Die weißen Hacker

Wie Cybersecurity-Experten Videolösungen auf Herz und Nieren prüfen

Seite 3

Das hässliche Entlein war einmal

So wird Videosicherheit zur strategischen IT-Komponente

Seite 7

Wenn die Kamera nach Hause telefoniert...

Auf 43 Milliarden Euro wurde der Schaden durch Cyberangriffe für 2017 und 2018 beziffert. Zum Beispiel wird alleine der Siemens-Konzern 1000-mal angegriffen – pro Tag*! Dabei wird die Rolle der Videosicherheitssysteme als mögliche Schwachpunkte von vielen Anwendern unterschätzt. Sehr zur Freude der Angreifer – das zeigen prominente, IP-Kamera-basierte Attacken wie etwa Carbanak, Mirai oder Persirai in den vergangenen Jahren. Aber auch Videomanagement-Systeme und Prozessoren werden attackiert.

** Quelle: Wirtschaftswoche*

Seite 2

Sicherheit beim Hersteller

Trusted Advisor oder Unsicherheitsfaktor?

Gerade in so sensiblen Bereichen wie der Sicherheitstechnik geht es nicht allein um die technische Lösung. Kunden möchten wissen, „mit wem sie es zu tun haben“. Einige Indikatoren können entscheidende Hinweise auf die Vertrauenswürdigkeit eines Herstellers geben.

Seite 8

Sicherheit bei der Planung

In Rekordzeit zur Videosicherheit in neun Fußballstadien

Weltweit vertrauen Unternehmen aller Branchen auf Videosicherheitstechnik von Dallmeier. Ausschlaggebend ist neben den technischen Vorteilen oftmals auch ein ganz anderer Aspekt: der besondere Ansatz des deutschen Herstellers bei der Projektplanung und -umsetzung.

Seite 6

Wenn die Kamera „nach Hause telefoniert“

VIDEOTECHNIK IST OFT DAS STIEFKIND DER CYBERSECURITY

Nicht schlecht durften die Sicherheitsbeauftragten zahlreicher Banken in verschiedenen Ländern im Jahre 2013 gestaunt haben, als ihnen russische Hackergruppen im Zuge der Kampagne „Carbanak“ einen dreistelligen Millionenbetrag „stibitzten“: Bei diesen Angriffen wurden Überwachungskameras innerhalb der Finanzinstitute kompromittiert um Bildschirminhalte und Tastatureingaben auszuspähen, Mitarbeiter z. B. über Namensschilder/Mitarbeiterausweise als Ziel für Spear-Phishing zu identifizieren, sowie Gewohnheiten und Reaktionen der Mitarbeiter in Erfahrung zu bringen.

In den Jahren 2016 und 2017 erlangten dann mit „Mirai“ und „Persirai“ zwei weitere Angriffe traurige Berühmtheit. Bei beiden ging es um das Lahmlegen zentraler IT-Dienste durch großangelegte „Distributed-Denial-of-Service-Angriffe“ (DDoS). Mirai und Persirai sind Botnetze, die ausschließlich aus IP-Kameras bestehen. Im Fall von Persirai insgesamt mehr als 1000 verschiedene Kameramodelle.

Mit der Gerätesuchmaschine Shodan fand der Sicherheitshersteller Trend Micro weltweit insgesamt rund 120.000 IP-Kameras, die sich theoretisch dem Persirai-Botnetz hinzufügen lassen. Laut Trend Micro wissen vermutlich viele der betroffenen Nutzer gar nicht, dass ihre Kameras über das Internet angreifbar sind.

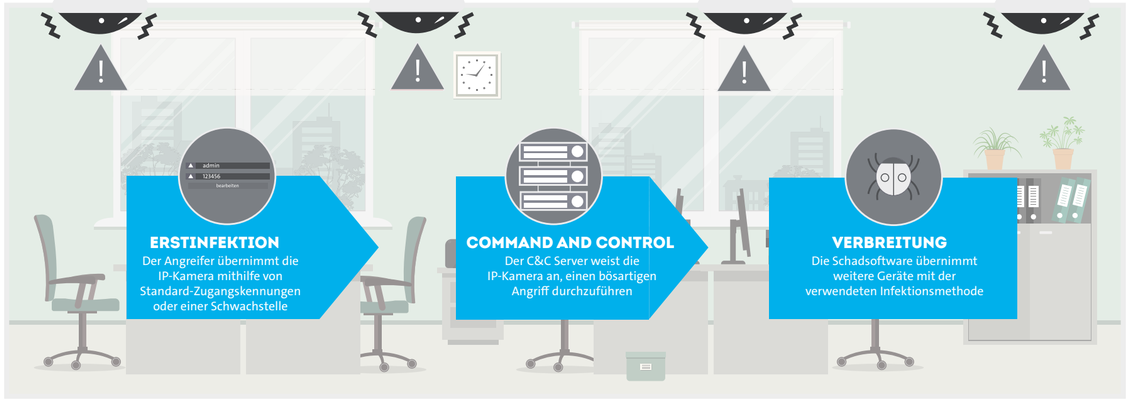
Der Angreifer kommt gerne einmal durch die Hintertür

Eine IP-Kamera ist eben nicht nur eine Kamera, sondern ein voll vernetztes „IoT“-Device mit allen Möglichkeiten und Risiken, die diese komplexe Technik bietet. Die verbauten „Embedded Systems“ sind nun wie jedes vernetzte System prinzipiell angreifbar: Viele bauen bereits ab Werk automatisch Verbindungen zu externen Servern auf, etwa für Updates, Fernwartung oder zum Speichern von Daten in der „Cloud“. Diese Verbindungen unterlaufen die Firewall; der Anwender hat in der Regel keine Kontrolle darüber, welche Daten über diese Verbindungen transportiert werden. Bei manchen Geräten sind Hintertüren (sog. „Backdoors“) bekannt geworden, die versehentlich oder absichtlich eingebaut wurden. Mitunter werden Geräte auch gezielt von Geheimdiensten, Industriespionen oder der organisierten Kriminalität manipuliert. Solche kompromittierten Systeme stellen ein erhebliches Sicherheitsrisiko für das gesamte betroffene Netzwerk und Unternehmen dar.

Top 10 der angegriffenen Ports bei IoT - Q4/17

No.	Port	Prozent
1	23/tcp (Telnet)	43,1
2	80/tcp (HTTP)	31,6
3	443/tcp (HTTPS)	7,7
4	2323/tcp (Telnet)	7,2
5	445/tcp (SMB)	5,8
6	22/tcp (SSH)	1,9
7	1900/udp (UPnP)	0,9
8	8080/tcp (HTTP)	0,8
9	2222/tcp (SSH)	0,2
10	21/tcp (FTP)	0,2

Quelle: Symantec Internet Security Threat Report 2018



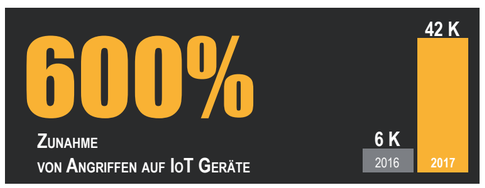
Der Angreifer nutzt Standard-Zugangskennungen oder eine Schwachstelle, um eine IP-Kamera zu übernehmen

Quelle: Darstellung in Anlehnung an Trend Micro

Anstieg der Attacken auf IoT-Geräte von 2016 auf 2017 um 600 %

IP-Kameras und digitale Videorekorder (DVR) gehören zu den am meisten angegriffenen IoT-Geräten. Dennoch sind auch Videomanagement-Systeme regelmäßig von Sicherheitslücken betroffen. Und selbst die in den Systemen verbauten Prozessoren sind grundsätzlich Angriffen ausgesetzt, wie die Prozessor-Sicherheitslücken „Spectre“ und „Meltdown“ eindrucksvoll bewiesen haben.

Eine Entwarnung ist nicht in Sicht: Laut dem „Internet Security Threat Report 2018“ von Symantec hat die Anzahl der Attacken auf IoT-Geräte alleine von 2016 auf 2017 um mehr als 600 % zugenommen. Interessant ist, dass diese Zahl in Relation steht zu „lediglich“ 13 % Zunahme der von Herstellern berichteten „Vulnerabilities“.



Top 10 der Gerätearten, die für Attacken missbraucht werden

No.	Gerät	Prozent
1	Router	33,6
2	DVR	23,2
3	Netzwerk	9,3
4	Satellitenschüssel	7,3
5	DSL / Kabel Modem	7
6	SOHO Router	4,7
7	NAS	3,6
8	Kamera	3,5
9	SPS (LPC)	3,4
10	Alarmanlage	1,9

Quelle: Symantec Internet Security Threat Report 2018

Videotechnik & Cybersecurity

Better safe than sorry!

Die Bedrohungslage für IoT-Systeme und damit auch für Videokameras stellt sich als sehr ernst zu nehmend dar. Dennoch gibt es einige wichtige Prinzipien, mit denen Kunden ihre Systeme wirksam vor Cyberrisiken schützen können.

Der passende Lösungsansatz

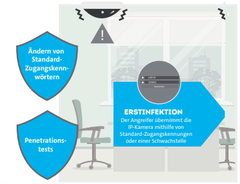
Schon bei der grundlegenden Planung von Videosicherheitssystemen können Unternehmen mit unterschiedlichen Lösungsansätzen potenziellen Cyberrisiken proaktiv begegnen: Von der kompletten physischen Trennung von Unternehmensnetzwerk und Videosystem, über VLAN und VPN bis hin zu einem sog. Video Security Gateway. Letztgenannter fungiert dabei als sichere Schaltzentrale und überwacht alle Verbindungen zwischen dem Unternehmensnetzwerk und dem Videonetzwerk.

Die Ingenieure und Netzwerkplaner vom deutschen Sicherheitsanbieter Dallmeier gehen hierbei mit besonderer Sorgfalt vor: Zusammen mit dem Kunden entwerfen sie eine Lösung für ihn, die nicht nur sicher ist, sondern sich in seine bestehende Netzwerkumgebung auch passend integrieren lässt.

Security by Design

Zudem sollten Kunden bei der Wahl von Sicherheitssystemen auf das Qualitätskriterium „Security by Design“ achten. Das bedeutet, dass diese Lösungen bereits ab Werk mit Datensicherheitsfunktionen ausgestattet sind. In diesem Kontext lässt sich bereits eine Menge Unheil abwehren, wenn Unternehmen die standardmäßig vergebenen Zugangsdaten ändern und der Hersteller umfassende Vorsorgemaßnahmen trifft. Bei Dallmeier gehört das Testen der eigenen Produkte auf Herz und Nieren zum integralen Bestandteil der Entwicklungsarbeit. Dazu beauftragt das Unternehmen in regelmäßigen Abständen externe, anerkannte IT-Sicherheitsprüfinstanzen zur Simulation von Hackerangriffen mittels Penetrationstests (siehe unten: Interview "Die weißen Hacker von cirosec").

So lässt sich auch die Eintrittswahrscheinlichkeit des zuvor geschilderten typischen Angriffs auf eine IP-Kamera enorm reduzieren:

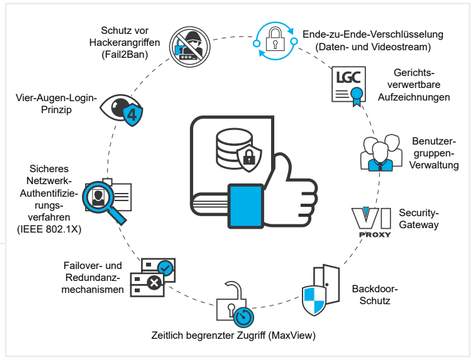


Einfach, aber effizient: Zugangserkennungen ändern und durch sichere Passwörter ersetzen sowie auf sorgfältige Entwicklungsarbeit beim Hersteller achten.

Zudem ist es sinnvoll, alle nicht benötigten Ports eines Videosystems zu deaktivieren. Bei Dallmeier-Produkten sind Telnet (Platz 1 der angegriffenen Ports!) und weitere unsichere Verbindungen per Standardeinstellung deaktiviert. Des Weiteren stellt das Unternehmen mit seinem kombinierten Datenschutz- und Datensicherheitsmodul ein umfangreiches Cybersecurity-Paket zur Verfügung, das nach der Leitlinie „Security by Design“ entwickelt wurde:

Zur Netzwerkabsicherung dienen die Authentifizierung gemäß IEEE 802.1X, eine Ende-zu-Ende Verschlüsselung mit TLS 1.2 / 256 Bit AES bei aktuellen Dallmeier-Systemen und die Funktion „ViProxy“, mit der Dallmeier Aufzeichnungs-Appliances als Security Gateway des Videosystems fungieren. Zudem erfolgt die Entwicklung sämtlicher Hard-, Soft- und Firmware-Lösungen im eigenen Haus, wodurch versteckte Zugangsmöglichkeiten durch Backdoors ausgeschlossen sind.

Auf Recording-Ebene gewährleisten das optionale „Vier-Augen-Prinzip“ bei der Sichtung von Aufzeichnungen, die Festlegung eines zeitlich begrenzten Zugriffs auf die Aufzeichnungen für verschiedene Benutzergruppen (MaxView) sowie eine hierarchisch gestaffelte Benutzergruppenverwaltung die Datensicherheit. Das sichere Erkennen und Verhindern von Verbindungsversuchen durch Hackerangriffe erfolgt über die „Fail2Ban“-Funktion, entsprechende Failover- und Redundanzmechanismen bei der Aufzeichnung schützen vor Datenverlusten. Schließlich stellt Dallmeier mit der LGC-Zertifizierung sicher, dass bei der Beweissicherung alle Kriterien für eine gerichtliche Verwertbarkeit erfüllt sind.



Die Datensicherheitsfunktionen des kombinierten Dallmeier Datenschutz- und Datensicherheitsmoduls

Cybersecurity als Prozess verstehen

Doch sind es nicht nur die technischen Funktionen, die Schutz vor Schwachstellen und Cyberattacken gewährleisten. Cybersecurity ist vielmehr ein fortlaufender Prozess. Konkret bedeutet dies: Sicherheitsupdates für Videosysteme sollten regelmäßig eingespielt und Sicherheitskonzepte unternehmensweit implementiert werden. Sämtliche Sicherheitsmaßnahmen gilt es ausführlich zu dokumentieren, bspw. über Checklisten und Leitfäden, wie z. B. Hardening Guides, die der Systemhärtung dienen.

Mitarbeiter und Führungskräfte sollten sich durch regelmäßige Schulungen auf dem neuesten Wissensstand halten. Denn nur wenn alle beteiligten Akteure an einem Strang ziehen und die technischen und organisatorischen Maßnahmen sinnvoll einsetzen, kann Videotechnik sicher sein und ihren Zweck erfüllen: Die Wettbewerbsfähigkeit und den Bestand eines Unternehmens langfristig zu sichern und seine Mitarbeiter zu schützen.

Die „Weißen Hacker“ von cirosec

Heute sind fast alle IoT-, IT- und Videosysteme sicherheitsrelevant. Umso wichtiger ist es, dass Hersteller unabhängige, externe Experten beauftragen, die die Systeme bereits in der Entwicklung auf Herz und Nieren testen. Das führende Unternehmen im deutschsprachigen Raum ist die Firma cirosec aus Heilbronn. Geschäftsführer und Gründer Stefan Strobel beantwortet im Interview Fragen von Video Extra.

HERR STROBEL, WELCHE BEDROHUNGEN SEHEN SIE BEIM THEMA VIDEOTECHNIK ALS AM GEFÄHRLICHSTEN AN?

Heutige Videotechniksysteme sind wie alle modernen vernetzten Geräte komplizierte Computersysteme, die ein Betriebssystem, zahlreiche Kommunikationsschnittstellen und viele Funktionen besitzen. Entsprechend können Hacker versuchen, die Kontrolle über die Systeme zu übernehmen, diese beliebig zu steuern oder sogar eigene Software auf die Systeme aufzuspielen. Aus einer Überwachungskamera, die zum Schutz des Unternehmens gedacht ist, kann so eine Hintertüre für Kriminelle werden. Die Hacker bekommen dadurch einen Zugang zum Firmennetz was in der Folge einen Diebstahl von Unternehmensgeheimnissen ermöglichen kann.

WIESO IST DAS THEMA SICHERHEIT BEREITS IN DER ENTWICKLUNG VON PRODUKTEN SO WICHTIG?

Sicherheitsprobleme, die erst nach der Produktentwicklung bekannt werden, können oft nicht mehr vollständig geschlossen werden, denn die Sicherheit eines IoT-Produktes beginnt schon mit dem sicheren Design der Hardware. Nur wenn die Hardware die nötigen Sicherheitsfunktionen besitzt, können die Anwendungsprogramme darauf aufbauen. Viele Verwundbarkeiten in IoT-Systemen entstehen aber auch durch Programmierfehler während der Entwicklung. Um diese zu vermeiden, müssen die Entwickler verstehen wie ein Angreifer vorgeht, um entsprechend sensibilisiert zu programmieren.

WELCHE LEISTUNGEN BIETET DIE FIRMA CIROSEC UND WAS BEDEUTET DAS FÜR DIE ENDANWENDER?

Wir beraten und unterstützen unsere Kunden in fast allen Bereichen der Informationssicherheit. Der größte Schwerpunkt liegt dabei auf der Prüfung von Systemen, sogenannten Penetrationstests. Dabei versuchen unsere Spezialisten mit den Techniken und Werkzeugen eines Hackers die IT-Systeme oder Produkte unserer Kunden anzugreifen. Dadurch werden Schwachstellen aufgedeckt, bevor ein Krimineller diese finden und echten Schaden anrichten kann.

GIBT ES VORSCHRIFTEN ODER ZERTIFIKATE, NACH DENEN UNABHÄNGIGE PENETRATIONS- UND ANDERE SICHERHEITSTESTS DURCHGEFÜHRT WERDEN?

Leider sind die offiziell aussehenden Zertifikate, die man heute manchmal auf Webseiten oder Produkten findet, mehr Marketing als wirkliche Bestätigungen der Sicherheit. Echte Standards, die auch international anerkannt sind, betreffen meist nur die Prozesse in einer Organisation. Es kommt daher vor allem darauf an, wer solche Prüfungen durchführt und wieviel Erfahrung dahintersteckt.

DIE PENETRATIONS- UND SICHERHEITSTESTS WERDEN JA VON DEN HERSTELLERN IN AUFTRAG GEGEBEN – WIE STELLEN SIE IHRE UNABHÄNGIGKEIT SICHER?

Unser guter Ruf im Markt ist uns sehr wichtig. Deshalb lehnen wir Prüfungsaufträge ab, bei denen wir den Eindruck haben, dass der Kunde gar nicht möchte, dass wir etwas finden beziehungsweise uns nicht genügend Zeit für eine angemessene Prüfung einräumt.

GIBT ES EINEN VORFALL AUS DEM BEREICH VIDEOSICHERHEIT, DER IHNEN BESONDERS IM GEDÄCHTNIS HAFTEN GEBLIEBEN IST?

Stefan Strobel,
Gründer + Geschäftsführer cirosec

Der vermutlich bekannteste Vorfall betraf sicher die im Herbst 2015 von einem Discounter verkauften Überwachungskameras. Viele Privatleute haben damals die kostengünstige Kamera gekauft und an ihr privates Netzwerk bzw. WLAN angeschlossen. Die Kameras haben sich selbständig am Internetrouter der Haushalte freigeschaltet und waren ohne Passwort im Internet erreichbar. Im Februar 2016 konnte man mit Hilfe der IoT-Suchmaschine Shodan über 10.000 ungeschützte Kameras finden und fernsteuern.

Nur ein ganzheitlicher Ansatz bietet Sicherheit!

Das sagen Kunden zur Datenschutz-Lösung von Dallmeier

das Stadtwerk.Donau-Arena: Peter Lautenschlager, Betriebsleiter

„Wir wollen zufriedene Besucher und Fans. Mit der Lösung von Dallmeier haben wir genau das richtige Maß an Datenschutz bei Gewährleistung eines Höchstmaßes an Sicherheit erhalten. Wir freuen uns, mit Dallmeier den richtigen Partner gewählt zu haben."

Datenschutz

- Auf „Privacy by Design" achten
- Kein Datenschutz ohne Datensicherheit
- Funktionen zur Erfüllung der DSGVO-Prinzipien

Seite 7

Cybersecurity

- Auf „Security by Design" achten
- Videotechnik erfüllt IT-Vorgaben
- Cybersecurity als Prozess verstehen

Seite 2 + 3

Das sagen Kunden zur Cybersecurity-Lösung von Dallmeier

Seven Luck Casino: IT-Manager, GKL

„Die Dallmeier Lösung gilt als eines der stabilsten Casino-Sicherheitssysteme, und auch bei unseren Tests hat sich die Technik bewährt."

Linz PlusCity Einkaufszentrum:
Michael Pechmann, Sicherheits- und Technikbeauftragter

„Wir gehen mit dem Thema offen um. Das wissen auch die Besucher zu schätzen und wir müssen nichts verstecken."

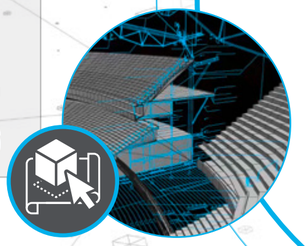
Dallmeier

#SichereVideotechnik

3D-Planung

- Datenschutzaspekte berücksichtigen
- Unsicherheiten bei der Implementierung minimieren
- „What we plan is what you get" – moderne 3D-Planung

Seite 6



IT-freundliche Videosysteme

- Wenige Systeme, geringe Komplexität
- Investitionssicherheit einfordern
- Integration in zentrale RZ-Ressourcen

Seite 7

Das sagen Kunden zum Dallmeier-Planungsansatz

Linz PlusCity Einkaufszentrum: Herbert Zachhuber, G4S

„Dallmeier bietet erstklassige Produkte. Es ist nur eine kurze Einweisungszeit nötig, durch die 3D-Projektierung und Vorinstallation im FAT-Center reduziert sich sowohl die Konfigurations- als auch die Montagezeit signifikant. Sämtliche Systeme sind schnell und innerhalb des geplanten Zeitraumes im Einsatz und ermöglichen sofort einen reibungslosen Ablauf."

das Stadtwerk.Donau-Arena: Peter Lautenschlager, Betriebsleiter

„Von Anfang an hatten wir eine ganz genaue Vorstellung davon, was wir später bekommen sollten. Und letztlich entsprachen sowohl Kamerablickwinkel als auch die Bildauflösungen über die gesamte Beobachtungsfläche exakt dem, was im 3D-Modell simuliert wurde. Das gab uns schon früh eine hohe Planungssicherheit, eine permanente Kostentransparenz und letztlich absolute Zufriedenheit nach der Umsetzung. Überraschend war, wieviel Planungs- und Projektarbeit durch die 3D-Technik bereits in einem sehr frühen Stadium „quasi nebenher" erledigt werden konnte."

Herstellervertrauen

- Herstellereinheitlichkeit
- Erfahrung und Roadmap
- „Made in Germany" als Gütesiegel

Seite 8

Das sagen Kunden zu Dallmeier als Hersteller

Your Homes Newcastle: Steven Studley, technischer Sachverständiger

„Die Polizei hat das Vertrauen in das System wiedergewonnen!"

Stadt Gaillard: Jean-Paul Bosland, Bürgermeister

„Dallmeier ist ein Unternehmen mit Visionen und legt bei der Entwicklung ihrer Produkte und Lösungen viel Wert darauf, dass Projekte über Jahre hinweg problemlos erweitert und skaliert werden können. Das schafft eine hohe Investitionssicherheit. Wir sind überzeugt, dass die Dallmeier-Technologie auch unseren zukünftigen Anforderungen gerecht wird."

Das sagen Kunden zum IT-freundlichen Ansatz von Dallmeier

Studio City Casino: Leroy Daniel, Executive Director MCE Surveillance

„Es gibt einige wichtige Integrationen, die Dallmeier einzigartig machen und mit denen wir unseren Geschäftsbetrieb besser schützen können. Dazu gehört die maßgeschneiderte Entwicklung von High-Level-Schnittstellen zu den Kernsystemen rund um unser Gebäude. Schnittstellen umfassen unter anderem die Spielautomaten, intelligente Kartenschlitten, Point-of-Sale, Zugangskontroll- und Einbruchssicherungssysteme sowie RFID-Jetons."

IKEA: Andrea Tomasekova, Administration Manager / CZ, HU, SK

„Die Dallmeier-Technik hat sich schon einmal bei einer größeren Erweiterung bewährt. Es ist ein gutes Gefühl zu wissen, dass die Videoanlage auch bei einer erneuten Modernisierung oder einem Ausbau wieder mitwachsen kann."

Frankfurt Airport: Maurice Dengel, Bereichsleitung Fraport & Rhein-Main

„Die Installation war einfach und unkompliziert."

„Und in letzter Minute soll noch ein Dach über den VIP-Bereich“

In Rekordzeit zur Videosicherheit in neun Fußballstadien

Welweit vertrauen Unternehmen aller Branchen auf Videosicherheitstechnik von Dallmeier. Ausschlaggebend ist neben den technischen Vorteilen oftmals auch ein ganz anderer Aspekt: der besondere Ansatz des deutschen Herstellers bei der Projektplanung und -umsetzung.

„What We Plan is What You Get“

Das Beispiel Stadien zeigt: Gleich ein ganzes Team aus Spezialisten ist bei Dallmeier für den Bereich 3D-Planung zuständig. Experten erstellen exakte dreidimensionale Simulationen der Kundenumgebung aus 2D- oder 3D-Plänen. Im „Notfall“ reichen sogar Fotos und „Google Maps“-Informationen. Im fertigen 3D-Modell wird dann die komplette Lösung exakt simuliert. Selbst Sichtfeldabdeckungen der Kameras, sog. Abschattungen, werden entdeckt und durch entsprechende Positionierung der Kameras oder Hinzufügen weiterer Komponenten beseitigt. Der Kunde erhält so eine exakte Planung seiner zukünftigen Umgebung, bei der alle Details berücksichtigt werden.

250 Pixel pro Meter als Vorgabe

Im Rahmen der 3D-Planung werden mit dem Kunden genau die Sicherheitsziele definiert. Beispielsweise ist bei Fußballstadien oftmals vorgegeben, dass in allen öffentlich zugänglichen Bereichen eine minimale Auflösungsdichte von 250 Pixel pro Meter (px/m) erreicht wird. Diese Kenngröße ist in einer DIN-Vorschrift geregelt und stellt sicher, dass unbekannte Personen eindeutig identifiziert werden können. Dank der 3D-Simulation ist es ein Kinderspiel, auch „im letzten Winkel“ die Vorgaben zu erfüllen: durch Farbcodierungen lässt sich genau sagen, wo der Wert erreicht wird und wo „nachgebessert“ werden muss.

Die Geschichte mit den VIP-Dächern

Beweisen konnte sich diese Vorgehensweise z. B. bei einem Projekt mit mehreren großen Fußballstadien: mitten in der Projektumsetzung sollten in allen Stadien noch zusätzlich Überdachungen für die obersten Tribünen angebracht werden, normalerweise angesichts des Zeitdrucks eine fast unmögliche Herausforderung für jeden Planer! Nicht so für das Dallmeier 3D-Projektplanungsteam: in weniger als zwei Tagen wurden die erforderlichen Änderungen bei Kameramodellen und Positionierung für alle Stadien umgesetzt.

Aus der Planung direkt auf die Baustelle

Ein besonderer Mehrwert der 3D-Planung sind die sog. „CamCards“ – genaue Konfigurationsdokumente für jede einzelne Kamera, die automatisch generiert werden. So weiß der Errichter vor Ort genau, welche Kamera wo, in welcher Höhe und in welchem Winkel montiert werden muss, welche IP-Adresse diese hat etc. Neben der enormen Zeitersparnis bedeutet dies vor allem auch Planungssicherheit – es lässt sich sehr genau vorhersagen, wieviel Aufwand für die Installation der Gesamtlösung nötig ist.

Keine Experimente: Test des Komplett-Systems bereits vor Auslieferung

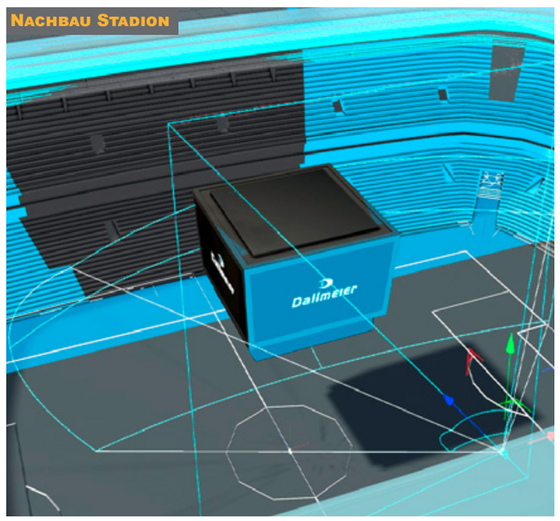
Gerade Entscheider aus der IT-Abteilung kennen das: Komplexe Systeme werden implementiert, und dann fängt die eigentliche Integrationsarbeit oft erst an. Nicht nur bei Fußballstadien ist dieser Ansatz natürlich mit Problemen behaftet. Dallmeier geht deshalb mit dem „Factory Acceptance Test (FAT)“ einen komplett anderen Weg: Sämtliche Lösungskomponenten werden im Dallmeier FAT-Centre zusammengestellt und die finale Umgebung wird im Live-Betrieb getestet bis alles reibungslos funktioniert.

Abdeckung von großen Arealen: vom Stadion bis zur Kölner Domplatte

Mit ausschlaggebend für die Entscheidung der Stadionbetreiber für Dallmeier war die patentierte Panomera®-Technologie. Die Panomera®-Kameras bieten bis zu acht Sensoren pro System und ermöglichen die Abdeckung größter Flächen bei definierter Pixeldichte mit deutlich weniger Kameras. Damit sinkt der Management-Aufwand, während der Bedienkomfort und damit auch die Sicherheit steigen. Beides führt zu einer signifikanten Verringerung der Gesamtbetriebskosten.

Dass die Systeme nicht nur für Fußballstadien geeignet sind, zeigen die zahlreichen weltweiten Projekte von Dallmeier mit Casinos in Macau, zahlreichen Logistikunternehmen oder auch im „Safe City“-Bereich wie etwa der Kölner Domplatte, wo seit 2016 insgesamt acht Panomera®-Systeme für Sicherheit sorgen und eine Lösung abbilden, für die über 100 klassische PTZ-Kameras erforderlich gewesen wären.

What we plan is what you get: 3D-Planung und Realsituation im Vergleich



Sichtfeldverdeckungen, hier durch einen Videowürfel, werden bereits in der Planung erkannt und berücksichtigt.

DSGVO

Die Welt ist NICHT untergegangen!

Jürgen Seiler, Geschäftsführer davidiT

Viele Kunden werden sich erinnern: An die vielen E-Mails von teilweise schon längst vergessenen Diensten, die darauf hingewiesen haben, dass die Datenschutzerklärung aktualisiert wurde. Oder an die unzähligen Sanduhren oder Timer, die den Eindruck erweckten, dass die Welt am 25. Mai 2018 untergehen wird. Genau an jenem Tag ist die neue Datenschutz-Grundverordnung in allen EU-Mitgliedsstaaten endgültig in Kraft getreten. Ähnlich wie bei der Jahrtausendwende hat sich der Sturm jedoch lediglich im Wasserglas abgespielt: die befürchteten „Abmahnwellen“ sind ausgeblieben und in Arztpraxen ist es nach wie vor erlaubt, beim Namen angesprochen zu werden.

Videosicherheit kommt in der DSGVO nicht vor

Vieles in der praktischen Umsetzung ist aber nach wie vor diffus. So beispielsweise auch das Thema Videosicherheit, zu der es in der DSGVO keine konkrete Regelung gibt. Vielmehr müssen die allgemeinen Vorschriften und Prinzipien daher auf die Videosicherheit übertragen werden, sofern mit entsprechenden Systemen personenbezogene Daten verarbeitet werden.

Wo finden Kunden Unterstützung?

Ein scharfer Blick auf das Kurzpapier Nr. 15 der Datenschutzkonferenz (DSK) beantwortet viele Fragen, was die formellen Anforderungen nach der DSGVO betrifft. Zudem zeigt der Quick Guide „Videosicherheit nach DSGVO“ von Dallmeier die wichtigsten DSGVO-Vorschriften im Kontext der Videosicherheit auf. Die nützliche Interpretationshilfe gibt dabei auch konkrete Empfehlungen und verweist auf technische Funktionen, die DSGVO-Konformität ermöglichen können. Anwender, die Detailinformationen zu den technischen Funktionen benötigen, finden diese in der Broschüre „Videosicherheit, Datenschutz und Datensicherheit“.

Hier finden Sie alle wichtigen Informationen rund um Videosicherheit & DSGVO

Nepper, Schlepper, Bauernfänger

AUGEN AUF BEI DSGVO-ZERTIFIKATEN!

Grundsätzlich unterstützt die EU freiwillige Zertifizierungsverfahren und Datenschutzsiegel bzw. Datenschutzzertifikate um die Transparenz zu erhöhen und um die Einhaltung der DSGVO zu erleichtern. Es besteht jedoch keine Pflicht zur Zertifizierung oder zum Einsatz zertifizierter Produkte. Zudem ist es nur möglich, Verarbeitungsvorgänge zu zertifizieren. Das bedeutet, dass Produkte, wie bspw. eine Überwachungskamera prinzipiell nicht zertifiziert werden können. Sowohl die Zertifizierungsstelle als auch die Datenschutzzertifikate selbst müssen von einer nationalen Akkreditierungsstelle oder von den Aufsichtsbehörden offiziell gemäß DSGVO akkreditiert sein. Das bedeutet, dass nicht jedes Datenschutzzertifikat notwendigerweise die gewünschte rechtliche Wirkung hat und potenzielle Geldbußen abschwächen kann.

Vom „hässlichen Entlein“ zur strategischen IT-Komponente

JEDER KUNDE INTEGRIERT VIDEOSICHERHEIT ANDERS

IT-Sicherheit und physische Sicherheit – Video, Brand, ZuKo, EMA – wachsen weiter zusammen. IT-Verantwortliche zählen dabei immer häufiger zu den wichtigsten Entscheidungsträgern für Videosicherheitstechnik. Oliver Koch, CIO bei Dallmeier, erläutert im Interview den nicht selten steinigen Weg.

HERR KOCH, IMMER HÄUFIGER FÄLLT VIDEOSICHERHEIT IN DIE VERANTWORTUNG DER IT-ABTEILUNGEN. WIE SEHEN SIE AUS IHRER SICHT ALS IT-LEITER DIESEN WANDEL?

Ausschlaggebend für diesen Paradigmenwechsel, wie ihn viele Unternehmen derzeit durchmachen, war natürlich der Wandel von der Analogtechnik zu IP-basierten Systemen. Damit war technisch die Einordnung in die IT-Struktur möglich. Wie so häufig sind pauschale Aussagen schwierig: Jedes Unternehmen ist anders, und wir beobachten sehr unterschiedliche Strategien.

WELCHE VORGEHENSWEISEN KÖNNEN SIE BEOBACHTEN?

Für manche Kunden, speziell größere Konzerne, ist Zentralisierung und Konsolidierung oberstes Gebot. Andere Unternehmen legen nach wie vor Wert auf eine komplette Trennung der Videosicherheit und der IT, da mit der Integration in zentrale RZ-Systeme ja nicht nur Vorteile verbunden sind. Das ist z. B. der Fall, wenn Wartungsarbeiten an zentralen Server- oder Storagesystemen Auswirkungen auf die Verfügbarkeit der Videosysteme haben und die Abstimmung zwischen IT und Sicherheitsabteilung nicht gut funktioniert.

WELCHE ANFORDERUNGEN STELLEN KUNDEN, DIE EINE MÖGLICHST ENGE EINBINDUNG IN ZENTRALE, STANDARDISIERTE IT-SYSTEME ERWARTEN?

Die Lösungen eines Herstellers müssen sich so flexibel wie möglich den Anforderungen anpassen können. Das bedeutet für Kunden, die einen sehr „IT-orientierten Ansatz“ verfolgen, dass Aufzeichnungs- und Managementsysteme sich nahtlos in virtuelle Serverumgebungen z. B. unter VMware einbinden lassen müssen. Ebenso wichtig sind die Integration in AD-Strukturen, Unterstützung aller gängigen Monitoringsysteme (z. B. Nagios, PTRG, Solarwinds etc.) durch SNMP oder die Einbindung in ERP-Systeme für Business Intelligence-Aufgaben. Auch Integration in Cloud-Dienste (z. B. Azure, AWS) werden von diesen Kunden zunehmend nachgefragt.

ANDERE KUNDEN SUCHEN BEWUSST NACH „STAND-ALONE“-LÖSUNGEN MIT HOHER HERSTELLEREINHEITLICHKEIT. WAS IST DAMIT GEMEINT?

Für viele unserer Kunden ist ein „autonomer Betrieb“ der Videosicherheitssysteme wichtiger als die Nutzung zentraler Ressourcen. Man möchte ganz bewusst eigenständige Systeme z. B. mit dedizierter Aufzeichnungshardware. Ein Argument ist dabei häufig Datenschutz und Datensicherheit. Hier erwarten Kunden bei Lösungen „aus einer Hand“ eine bessere Abstimmung der Einzelsysteme aufeinander und damit ein höheres Maß an Sicherheit. Nicht selten ist dieser Ansatz auch – im Gegensatz zur verbreiteten Meinung – kostentechnisch die günstigere Variante. Wichtig für uns als Hersteller ist, dass wir beide Anforderungsprofile gleichermaßen bedienen können.

WELCHE WEITEREN TRENDS SIND AUS IHRER SICHT ZUKUNFTSTRÄCHTIG?

Ebenfalls mehr Flexibilität erwarten Kunden bei der Art der Beschaffung. Hier sprechen wir zunehmend mit IT-, Security- und Einkaufsverantwortlichen, die sich für Subscription- oder sogar Betreiber- bzw. „as-a-Service“-Modelle oder gemischte Varianten bei der Beschaffung interessieren. Vorteile sind ganz klar mehr Flexibilität und eine andere Kostenstruktur – Stichwort Betriebs- statt Investitionskosten. Ein weiterer Trend ist die zunehmende Wahrnehmung von Videotechnik als IT-Infrastruktur-Komponente, die weit mehr kann als Videoüberwachung. Denken Sie nur an die Erfassung von Videodaten zur Prozessoptimierung oder Verbesserung von Marketingaktivitäten.

Oliver Koch, CIO Dallmeier

Ein sehr positives Feedback gerade aus IT-Abteilungen erhalten wir auch zu unserem Planungsansatz: Die Kombination von 2D- bzw. 3D-Planung mit unserem „Factory Acceptance Test“ bietet dem Kunden einen „Plug and Play“-Ansatz mit einer äußerst zuverlässigen Planung und fast 100-prozentige Berechenbarkeit der Implementierung. Etwas, das viele IT-Verantwortliche aus ihrer Erfahrung so nicht kennen.

Sicherheit + Herstellervertrauen

SO WIRD DER HERSTELLER ZUM „TRUSTED ADVISOR“

Gerade in so sensiblen Bereichen wie der Sicherheitstechnik geht es nicht allein um die technische Lösung. Kunden möchten wissen, „mit wem sie es zu tun haben“. Einige Indikatoren können entscheidende Hinweise auf die Vertrauenswürdigkeit eines Herstellers geben.

Wirtschaftliche Situation des Herstellers
Eine Übernahme des Technologieanbieters muss nicht zwangsläufig negative Auswirkungen haben. Dennoch steigt dadurch natürlich die Unsicherheit, ob z. B. das Lösungsportfolio weiterentwickelt wird oder die Betreuungsqualität bleibt. Finanziell eigenständige Unternehmen können hier Vorteile bieten.

Politische Rahmenbedingungen
Im August 2018 verabschiedeten Kongress und Senat der USA ein Gesetz, das öffentlichen Auftraggebern in den USA Kauf und Einsatz von Systemen zweier großer asiatischer Hersteller untersagt. Für die Kunden bedeutet dies einen bedeutenden Mehraufwand durch die notwendige Neubeschaffung und -implementierung. Die Auswahl eines Anbieters sollte gerade im Hinblick auf Industriespionage und politischer Einflussnahme durchaus kritisch auch unter dem Aspekt des Herkunftslandes und dessen politischer Struktur erfolgen.

„Single Source of Trust“
Unter dem Begriff der „Herstellereinheitlichkeit“ lässt sich der Ansatz vieler Kunden zusammenfassen, möglichst alle Komponenten von einem Hersteller einzusetzen. Die Entwicklung unter einem Dach ermöglicht häufig eine weitergehende Integration der Elemente unter Sicherheitsaspekten. Vom Gegenkonzept des „Best of Breed“ erwarten Kunden, jeweils die beste Einzellösung im Markt zu erhalten. Für beide Ansätze gibt es valide Argumente.

Erfahrung und Langfristigkeit
Wichtig in einer vertrauensvollen Partnerschaft ist für viele Kunden auch die Erfahrung, die ein Hersteller mitbringt, dessen Qualitätsbewusstein, aber auch die Ernsthaftigkeit mit der er seine zukünftigen Ziele verfolgt. Indikatoren dafür können die Fertigungstiefe sein – wieviel der eigenen Entwicklung und Produktion findet im eigenen Hause statt, aber auch Dinge wie Roadmaps und Zukunftsinvestitionen.

„Sicherheit braucht Vertrauen. Deshalb legen wir Wert darauf, qualitativ hochwertige Lösungen zu entwickeln, die zum einen eine hohe Lebensdauer aufweisen, zum anderen aber dank ihrer offenen Plattformen auch Drittsysteme sowie neue Entwicklungen und Innovationen integrieren können. Die Erfahrung speziell der letzten Jahre zeigt zudem, dass Herstellereinheitlichkeit einen wertvollen Beitrag zu einer verbesserten Gesamtsicherheit leisten kann. Das in der DSGVO verankerte Grundprinzip „Security by Design“ verfolgen wir bei Dallmeier bereits seit 35 Jahren.“

Dieter Dallmeier
Founder & CEO, Dallmeier electronic

„Die Polizei hat das Vertrauen in das System wiedergewonnen!“

Steven Studley, technischer Sachverständiger, Your Homes Newcastle

Machen Sie den Anbieter-Check:

7 Fragen für das Gespräch mit dem Hersteller

WIE NEUTRAL ERFOLGT DIE PRÜFUNG DER SICHERHEIT?

Wie viel Wert legt der Hersteller auf neutrale Bewertung des Sicherheitsniveaus seiner Systeme, z. B. durch unabhängige Penetrationstests während und nach der Entwicklung?

WIE TIEF IST DIE WERTSCHÖPFUNG IN FERTIGUNG UND ENTWICKLUNG?

Eine tiefe Integration erhöht meist die Qualität von Gesamtlösungen und damit den Kundennutzen. Welcher Anteil des Portfolios kommt aus dem eigenen Hause? Wo findet die Produktion statt?

LEBT DER HERSTELLER DEN PLATTFORMGEDANKEN?

Bei allen Trends zu mehr „Herstellereinheitlichkeit“ ist es bei der heute vorhandenen Komplexität sehr wichtig, dass Systeme offen sind, Standards wie z. B. ONVIF umfassend unterstützt werden und sich Drittsysteme leicht integrieren lassen.

WIE GUT KENNT DER HERSTELLER TECHNIK UND BRANCHE?

Jahrelange Erfahrung in der Videosicherheitstechnik und tiefe Branchenkenntnis lassen sich nicht so leicht ersetzen. Der Hersteller sollte diese Kompetenz ausreichend darstellen können.

BIETET DER HERSTELLER KOMPLETTLÖSUNGEN ODER BAUSTEINE?

Gerade aus Sicherheitsaspekten hat der „Alles aus einer Hand“-Ansatz Vorteile, da die einzelnen Elemente optimal aufeinander abgestimmt sind.

GIBT ES EINE DOKUMENTATION DER MASSNAHMEN UND FUNKTIONEN FÜR DATENSICHERHEIT UND DATENSCHUTZ?

Die DSGVO droht mit rigiden Maßnahmen bei Missachtung ihrer Prinzipien. Ein Hersteller sollte glaubhaft und nachvollziehbar dokumentieren, wie der Themenkomplex Datenschutz und Datensicherheit adressiert wird.

MIT WEM HABE ICH ES ZU TUN?

Es sollten bei der Herstellerwahl auch Aspekte wie z. B. eine mögliche politische Einflussnahme im Herkunftsland oder die wirtschaftliche Abhängigkeit von Shareholder-Interessen mitberücksichtigt werden.

Vereinbaren Sie einen Termin mit einem unserer Experten

Informieren Sie sich über Dallmeier in einem Kurzporträt auf YouTube

Hier finden Sie weitere Informationen rund um Videotechnik & Cybersecurity

IMPRESSUM

Herausgeber: Dallmeier electronic GmbH & Co.KG, Bahnhofstr. 16, 93047 Regensburg, info@dallmeier.com, www.dallmeier.com
Ansprechpartner: Pressestelle Dallmeier, presse@dallmeier.com
Bildnachweise: Shutterstock, Fotolia. Bei allen anderen Motiven liegt das Copyright bei Dallmeier electronic GmbH & Co.KG
Layout und Redaktion: Dallmeier electronic GmbH & Co.KG
Gesamtverantwortlicher: Georg Martin M.A., CCO, Dallmeier Unternehmensgruppe

Weitere Informationen

Made in Germany