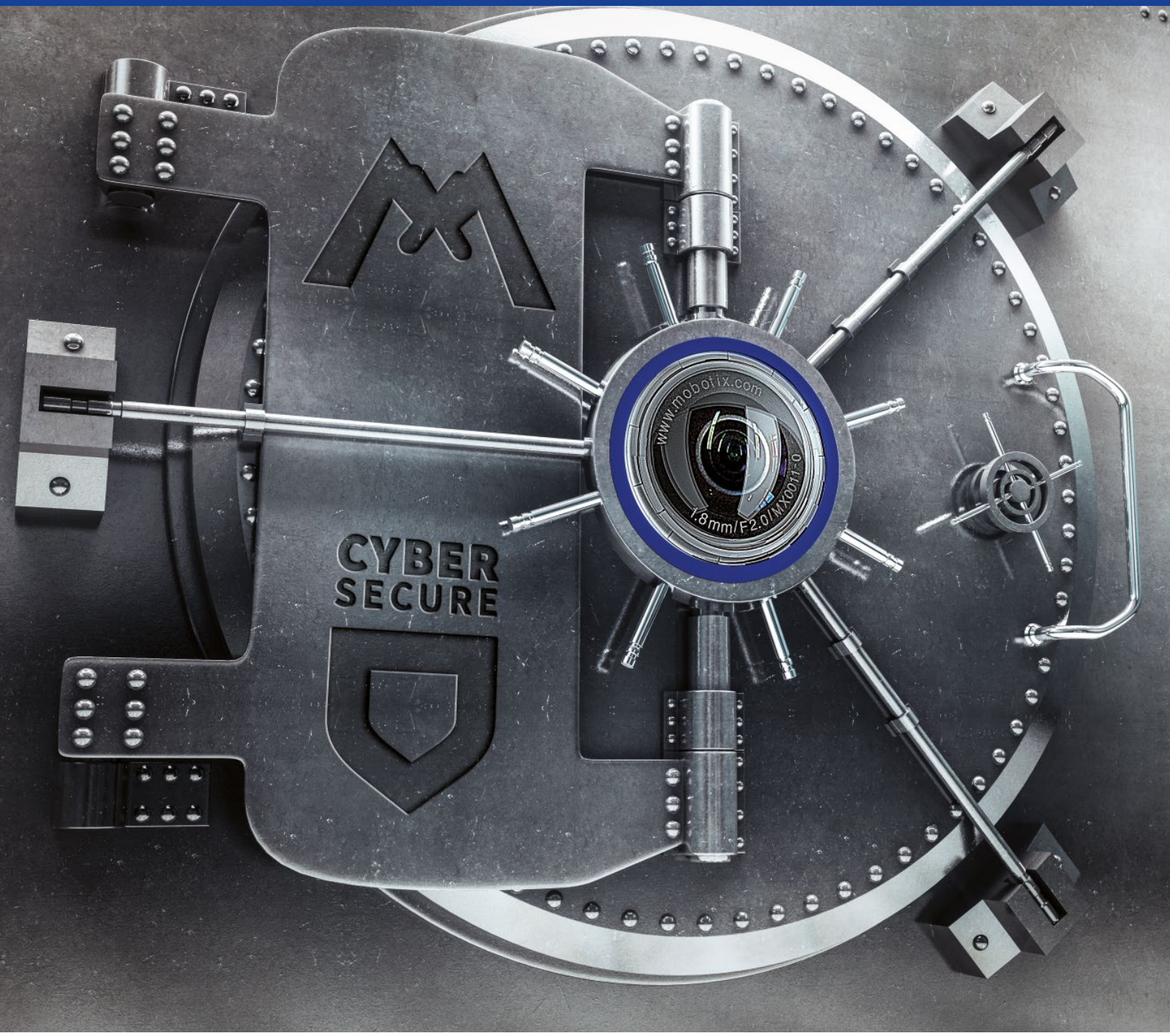
Cybersicherheit in Video-Sicherheitssystemen

Whitepaper



BeyondHumanVision

MOBOTIX

Einleitung

Ob im Gebäudeschutz, in der industriellen Fertigung oder als Garant für persönliche Sicherheit – Videosysteme sind fest in unserem Alltag verankert und tragen zum Wohlergehen von Milliarden Menschen bei. Familien können den Wochenendeinkauf unter dem schützenden Auge der Kamera erledigen, Manager analysieren vom Büro aus Produktmängel im Fertigungsbetrieb, und besorgte Eltern behalten ihr schlafendes Kind im Blick.

Was sind die wichtigsten Wachstumstreiber?		
1	Wachsende Sicherheitsbedenken	58 %
2	Verbesserungen bei der Videoanalyse	51 %
3	Verfügbarkeit von IP-Netzwerken	50 %

Diese Entwicklung wurde nicht zuletzt durch den rasanten Fortschritt in der Informations- und Kommunikationstechnologie begünstigt. Wo früher noch das Bildmaterial per Hand ausgewertet wurde, erledigen inzwischen intelligente Systeme und Sensortechnik die Arbeit und lösen automatisch Alarme oder Aktionen aus. Videotechnologie wird nicht länger nur passiv konsumiert. Der Grad der Automatisierung ist so weit fortgeschritten, dass anhand des beobachteten Geschehens eigenständig Maßnahmen ergriffen werden können.

Ein bekanntes Beispiel ist die elektronische Nummernschilderkennung im Rahmen der Lkw-Maut. Komplexere Lösungen werden unter anderem eingesetzt, um winzige Defekte in Maschinen zu identifizieren, bevor diese den Dienst versagen. Selbst in traditionellen Kontexten wie beim Einsatz von Videotechnik in Ladengeschäften tragen innovative Elemente wie „People Counting“ und Analysen des Einkaufsverhaltens dazu bei, den Aufbau von Geschäften zu optimieren oder neue Shoppingcenter zu planen.

Cisco schätzt, dass Videoinhalte für Unterhaltungs- und geschäftliche Zwecke bis 2020 rund 80 Prozent des Datenverkehrs im Internet ausmachen – die Nachfrage steigt also rasant.[1] Und dank kleineren, billigeren und energieeffizienteren Kameras ist die Technologie inzwischen für jedermann erschwinglich. Hinzu kommt, dass sich die Übertragung von Videodaten in Zeiten des Internets und schneller Mobilfunknetzwerke immer unkomplizierter gestaltet. Videotechnologie im Allgemeinen und Videosicherheit im Besonderen wird überwiegend ein positiver Effekt auf die Gesellschaft zugeschrieben, da sie sinkende Kriminalitätsraten bedingt und die persönliche Freiheit durch die Sicherung unserer Lebensumgebung stärkt. Mit der universellen Nutzung von Videotechnologie geht allerdings auch ein erhöhtes Risiko einher – und zwar in Gestalt von kriminellen, terroristischen und anderen Gruppierungen, die Video-Sicherheitssysteme sabotieren und für illegale Machenschaften nutzen wollen.

Risiken ungesicherter Videoanlagen und IoT-Geräte

In der Vergangenheit waren Angriffe gegen Video-Sicherheitsnetzwerke eine Seltenheit. Schließlich handelte es sich meist um geschlossene, in Privatbesitz befindliche Systeme, die direkt mit einer Leitstelle vor Ort verkabelt waren. Darüber hinaus verfügten Kameras der alten Schule über einen festverdrahteten Aufbau und waren mit simpler Firmware ausgestattet, die lediglich in der Lage sein musste, ein Videosignal über ein Koaxialkabel zu senden. Die Zeiten haben sich jedoch grundlegend geändert. Moderne Videokameras sind leistungsstarke Computer, die mit Software und einem digitalen Bildsensor ausgestattet sind. Dank der Ausbreitung des Internets und gesunkenen Anschaffungskosten sind Video-Sicherheitssysteme zunehmend über IP-Netzwerke zugänglich.

Damit einher gehen immer komplexere Prozesse, Softwareprotokolle und Authentifizierungsmechanismen. Der technische Fortschritt hat jedoch auch seinen Preis: mehr Schlupflöcher für Angreifer. Diese Problematik kennt man bereits vom Onlineshopping oder Kreditkartenbetrug. Doch auch im Videobereich steht das Thema schon seit längerem auf der Agenda. Bereits seit über einem Jahrzehnt weisen Sicherheitsexperten auf Schwachstellen in Kameras hin[2] – sowohl bei führenden internationalen Herstellern als auch bei kleineren regionalen Marken. Die Liste der Sicherheitsrisiken gibt großen Anlass zur Sorge:

- Angriffe, die Schutzmechanismen über ein standardmäßiges Benutzerkonto außer Kraft setzen, um Admin-Rechte auf einer Kamera zu bekommen
- Exploits, die die Benutzerauthentifizierung umgehen, indem sie festcodierte, vom Gerätehersteller als „Hintertür“ in die Kamera eingebaute Anmeldedaten nutzen
- Ausführung von Schadcode auf dem Gerät, ohne dass eine Authentifizierung erforderlich ist, indem Schwachstellen im Streamingprotokoll RTSP ausgenutzt werden
- Sicherheitslücken, die eine Authentifizierung durch den Kamerabediener umgehen, sodass sich ein Angreifer direkten Zugang zu den Konfigurationsdateien verschaffen kann
- Exploits, dank denen ein Angreifer das Gerätepasswort zurücksetzen und Konfigurationsdateien modifizieren kann, um auf Kernfunktionalität der Kamera zuzugreifen
- Angriffe, bei denen Drittparteien Video-Livestreams abfangen können, die über ein privates Netzwerk oder das Internet gesendet werden

Unter diesen Problemen leiden nicht zuletzt kleinere Firmen, die Technologie von großen Herstellern lizenzieren. Die Folge sind Schwachstellen in Millionen von Geräten. Obwohl die führenden Kamerahersteller Patches zur Problembehebung veröffentlichen, wird das Problem von vielen kleineren Unternehmen einfach ignoriert. Darüber hinaus müssen Updates anschließend noch manuell vom Eigentümer der Videoplattform implementiert werden – eine Tatsache, derer sich viele nicht bewusst sind. Die

Problematik betrifft auch Heimanwender, die Videosicherheitssysteme über den Einzelhandel bezogen haben und größtenteils in ungepatchte Anlagen vertrauen.

Gezielte Angriffe und Botnets

Es ist der Stoff, aus dem klassische Hollywood-Blockbuster gemacht sind: Ein Videosystem, das kritische Infrastruktur oder gar eine ganze Stadt schützen soll, wird sabotiert und komplett lahmgelegt. Doch ist diese Vorstellung wirklich so weit hergeholt? Viele Anbieter von Kamerasystemen nutzen für Streaming, Benutzerauthentifizierung und Datenspeicherung dieselben Softwarebibliotheken. Hier bietet sich ein Ansatzpunkt für gewiefte Angreifer, um Verbrechen zu planen und Angst und Schrecken zu verbreiten.

Ein weiterer Schwachpunkt ist der Netzwerkaspekt: Haben sich Cyberkriminelle erst einmal Zugang zu einem vernetzten Gerät wie einer Kamera verschafft, können sie ihre privilegierte Stellung ausnutzen, um andere Geräte im Netzwerk zu kompromittieren. Fakt ist, dass Kameras und anderes Equipment vermehrt mit dem Internet der Dinge (IoT) verbunden sind. Auch wenn derartige Systeme in der Regel über durchdachte Schutzmechanismen verfügen, führt die Notwendigkeit, auf IoT-Geräte zuzugreifen, zu einem erhöhten Risikopotenzial. Doch ein direkter Angriff auf Kameras ist nicht das einzige Problem. In jüngerer Vergangenheit wurden Fälle beobachtet, in denen Kameras gekapert und im Rahmen von Distributed-Denial-of-Service-Angriffen (DDoS) als Waffe eingesetzt wurden.

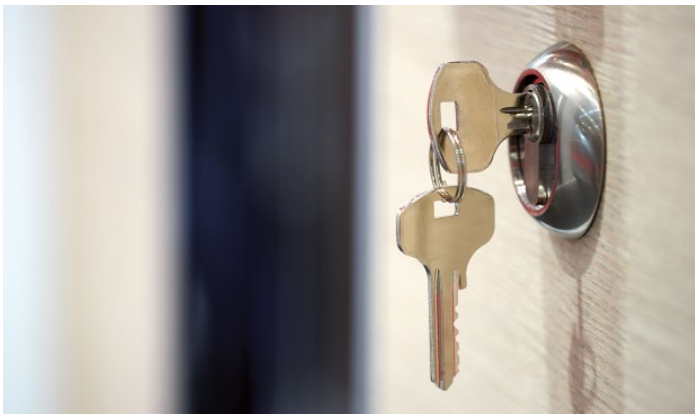
Für eine breit angelegte DDoS-Attacke im Oktober 2016, von der Twitter, Amazon, Tumblr, Reddit, Spotify und Netflix betroffen waren, zeichnete in Teilen ein Mirai-basiertes Botnet verantwortlich. Laut Allison Nixon, Forschungsdirektorin beim Mediengroßhändler Flashpoint, bestand das Botnet primär aus digitalen Videorekordern und IP-Kameras, die vom chinesischen Unternehmen XiongMai Technologies hergestellt wurden. XiongMai verkauft seine Bauteile an Anbieter, die sie dann wiederum in ihren eigenen Produkten verbauen. Zehntausende dieser Geräte sind nun zu gefährlichen Waffen im Cyberkrieg umfunktioniert worden.[3]

Politik und Rechtslage

Gartner, Cisco und anderen Branchengrößen zufolge wird die Zahl der mit dem Internet vernetzten Geräte bis 2020 explosionsartig auf 25 bis 50 Milliarden ansteigen.[4] Länderregierungen und internationalen Aufsichtsbehörden bereitet diese Entwicklung naturgemäß Kopfschmerzen. Im Gegensatz zu Radiosendern, TV-Stationen oder Kraftfahrzeugen bewegt sich IoT-Technik noch in einer rechtlichen Grauzone. Gesetzlich verpflichtende Standards zur Sicherheit von IoT-Geräten? Bisher Fehlanzeige. Was passiert also, wenn ein Gerät gehackt oder als Einstiegspunkt für einen Angriff auf Dritte genutzt wird? Cyberkriminalität kann in den meisten Ländern strafrechtlich verfolgt werden, wenn Opfer und Täter identifizierbar sind. In der gegenwärtigen Zeit verselbstständigt sich Technologie jedoch in zunehmendem Maße. Damit steigt das Risiko, dass ungesicherte Geräte massenhaft Viren anziehen, welche dann wiederum in Video-Sicherheitssystemen auftauchen, wo sie nur schwer ausfindig gemacht oder beseitigt werden können.

Finanzielle und strafrechtliche Haftung

Dann ist da das Problem der Haftung. Eigentümer von Video-Sicherheitssystemen profitieren in der Regel von geringeren Versicherungsbeiträgen und einem höheren Schutz vor kriminellen Übergriffen. Wird jedoch ein Videosystem aufgrund einer Sicherheitslücke lahmgelegt und ein Verbrechen begangen, das nicht per Kamera dokumentiert wird, kann die Auszahlung von Entschädigungssummen unter Umständen verweigert werden, da der Versicherte seiner Sorgfaltspflicht nicht nachgekommen ist. Sollte in diesem Fall das Opfer den Kamerahersteller verklagen? Oder den Wartungsdienstleister der Anlage? Würde bei einem öffentlichen Sicherheitsvorfall die



Lokalregierung zur Rechenschaft gezogen werden? Es gibt viele Fragen im Hinblick auf Sicherheitslücken in Video-Sicherheitsanlagen und nur wenige Erfahrungswerte. So verwundert es kaum, dass in der Branche eine große Ungewissheit vorherrscht.

Datenschutzbedenken

Während die finanziellen und strafrechtlichen Aspekte bei einem Hackerangriff auf Video-Sicherheitssysteme noch hitzig diskutiert werden, hat die Datenschutzgesetzgebung in den meisten Industrieländern längst Kontur angenommen. Generell müssen alle personenbezogenen Daten zu Gesundheit, Finanzen und anderen Kriterien auf sichere Art und Weise erfasst und gespeichert werden. Das gilt auch für Videodaten. Stets ist das Bildmaterial sicher und für Dritte unzugänglich aufzubewahren. Im Falle eines Cyberangriffs auf Video-Sicherheitstechnik besteht ein hohes Risiko, dass personenbezogene Informationen wie Bilder und andere Daten gestohlen oder

unbefugt offengelegt werden. Dies würde die Datenschutzrechte von Anwendern verletzen und könnte rechtliche Konsequenzen für den verantwortlichen Datenverarbeiter nach sich ziehen.

Die Politik tritt auf den Plan

Regierungen weltweit erarbeiten Lösungen, damit die neue Welle an IoT-Geräten nicht zu einem gigantischen Sicherheitsrisiko wird. In Europa haben führende Köpfe der EU-Kommission einen Zertifizierungsprozess für IoT-Geräte angeregt, der Anwender effektiver schützen soll. Darüber hinaus hat die Kommission die "Alliance for Internet of Things Innovation" mitbegründet, welche sich aus führenden Technologieherstellern aus dem Energie-, Automobil- und Gesundheitssektor zusammensetzt und gemeinsame Leitlinien für den Umgang mit dem Internet der Dinge erarbeiten soll. Jenseits des Atlantiks hat das US-Heimatschutzministerium Empfehlungen für ein sicheres Internet der Dinge veröffentlicht.[5] Behandelt werden unter anderem Schlüsselkonzepte wie „Security by Design“ sowie die aktive Förderung von Sicherheitsupdates und des Managements von Sicherheitslücken, wobei Sicherheitsmaßnahmen anhand des möglichen Schadensausmaßes priorisiert werden. Dennoch fehlt ein globaler oder industrieweiter Sicherheitsstandard, wie es ihn etwa im Payment-Bereich in Form des PCI-DSS gibt. Somit unterliegt die Sicherheit von IoT-Geräten länderspezifischen Richtlinien und Regulierungsauflagen, die in Umfang und Wirkung stark variieren.

Welche Antworten liefert MOBOTIX auf diese Problematik?

Als ein Marktführer der digitalen Video-Sicherheit nimmt MOBOTIX eine Ausnahmestellung ein, da wir unsere komplette Software selbst entwickeln. So sind wir nicht nur in der Lage, Produkte ganz nach unseren Vorstellungen anzubieten, sondern setzen auch in Sachen Sicherheit Maßstäbe. Da die Softwareentwicklung in Unternehmenshand liegt, ist MOBOTIX weniger anfällig für Szenarien, in denen unausgereifte Drittanbietersoftware und -hardware zu Sicherheitsverletzungen führt. In Bereichen, wo wir gängige Branchenstandards wie ONVIF nutzen, haben wir uns verpflichtet, verfügbare Patches zu veröffentlichen, sobald sie erfolgreich mit unseren Produkten getestet wurden. Indem wir dieselbe Software für alle Kameramodelle verwenden, können unsere internationalen Kunden Geräte-Firmware leichter auf dem neuesten Stand halten.

Unsere Produkte sind von Haus aus sicher, was sich in in vielen Bereichen zeigt:

Sicheres Betriebssystem und Updates

Die Sicherheitsphilosophie von MOBOTIX ist schon im Betriebssystem und im Application Stack der Kamera klar erkennbar. Alle Geräte arbeiten auf Basis eines modifizierten Linux-Betriebssystems, das auf nicht benötigte Standarddienste und -module verzichtet. Kritische Linux-Module wie die Authentifizierung wurden komplett umgestaltet. So können wir sicherstellen, dass diese Module nicht für gängige Exploits oder Code-Injection-Techniken anfällig sind. Unsere Software ist nicht quelloffen und wird durch zusätzliche Sicherheitsmechanismen geschützt. Zudem ist jedes Update für Geräte-Firmware und Softwarekomponenten verschlüsselt und digital signiert, um Manipulation vorzubeugen.

Sichere Kamerakonfiguration

Der Zugriff auf die Bedienschnittstelle zur Kamerakonfiguration ist nur autorisierten Anwendern gestattet. In jedem System können abgestufte Rechte für verschiedene Benutzergruppen erstellt werden. Das bedeutet in der Praxis: Kameras von MOBOTIX speichern Anwenderpasswörter niemals als Klartext, sondern versehen diese mit einem komplexen Hash-Algorithmus (SHA-512). Gelangt eine Konfigurationsdatei in falsche Hände, wäre es extrem schwierig, das Passwort im Klartextformat zu extrahieren. Nicht benötigte Linux-Dienste werden deaktiviert, um Schwachstellen zu beseitigen und Angriffen vorzubeugen. Zudem gibt es kein undokumentiertes Telnet- oder Master-Passwort – Kameras von MOBOTIX werden über ein Webportal angesteuert und konfiguriert. Passwörter können in Privileged-Account-Managementlösungen wie BeyondTrust oder CyberArk gespeichert und mittels fortschrittlicher Zwei-Faktor-Authentifizierung gesichert werden.

Sichere Netzwerk- und Gerätekommunikation

Alle zwischen MOBOTIX Kameras und anderen Netzwerk-Hosts ausgetauschten Daten können verschlüsselt werden, um die Vertraulichkeit und Integrität der Datenströme zu gewährleisten. HTTPS (SSL/TLS) und Stammzertifikate werden in Einklang mit Best Practices von Branchengrößen wie dem SANS-Institut standardmäßig unterstützt. MOBOTIX bietet zudem integrierte Unterstützung zur Verwaltung eindeutiger X.509-Zertifikate auf jeder Kamera, damit Unternehmen Kameras und Türstationen sichern können, die über Systeme wie OpenVPN authentifiziert werden. Das bedeutet: Wird eine Kamera gestohlen oder gehackt, kann der Angreifer mit den Zugriffsdaten der kompromittierten Kamera nicht das übrige Kamerasystem infiltrieren.

Sichere interne Aufzeichnung und Manipulationsschutz

Alle Aufzeichnungen, die von der Kamera generiert werden, können vor der Speicherung verschlüsselt werden – angefangen vom Ringpuffer, der die in jede Kamera integrierte SD-Karte nutzt. MOBOTIX hat ein sicheres Datei-

system entwickelt. Wenn eine Kamera gehackt oder gestohlen wird, kann der Zugriff auf kameraintern aufgezeichnete Videodaten verweigert werden, wenn keine Administratorrechte vorliegen, die mittels der zuvor beschriebenen Konfigurationsprozesse geschützt werden. Jedes von einer MOBOTIX Kamera produzierte Bild kann mit dem passenden Zertifikat digital signiert werden, um eine Manipulation zu verhindern. Dementsprechend werden Aufzeichnungen auch vor Gericht als Beweismittel zugelassen.

Sicherheitsfunktionen	Standard-IP-Kameras	MOBOTIX
HTTPS (SSL/TLS) und Zertifikate	✓	✓
HTTP-Authentifizierung	✓	✓
Access Control Lists	✓	✓
Abgestufte Anwender- und Gruppenberechtigungen	⚠	✓
Intrusion Detection	✗	✓
Anti-Bot-Schutz	✗	✓
Verschlüsselte Aufzeichnungen	✗	✓
Verschlüsselte Videos & Messages	✗	✓
VPN-Client	✗	✓

Intrusion Detection

Trotz der genannten Sicherheitssysteme und -prozesse wäre es fahrlässig anzunehmen, dass Kameras von MOBOTIX von Cyberangriffen verschont blieben. Deshalb hat MOBOTIX in zusätzliche Maßnahmen investiert, um Manipulationsversuchen vorzubeugen. Dank der Implementierung bewährter Intrusion-Detection-Techniken meldet jede Kamera oder Türstation unbefugte Anmeldeversuche und Brute-Force-Angriffe über einen verschlüsselten Kanal. Zudem kann im Falle einer wiederholt gescheiterten Anmeldung die betreffende IP-Adresse automatisch gesperrt werden.

Fazit

Die Popularität von Videotechnologie in Sicherheitsanlagen sowie in zentralen Bereichen des öffentlichen Lebens hält unvermindert an. Folglich geraten verstärkt Aspekte wie die Zutrittskontrolle, das Umweltmonitoring und Analyseprozesse wie Gesichtserkennung in den Fokus von Cyberkriminellen.

Entwickler von Video-Sicherheitssystemen müssen gemeinsam mit Anlagenbedienern und Aufsichtsbehörden Lösungen entwickeln, wie ein höheres Maß an Sicherheit erreicht werden kann. Diese Verpflichtung besteht einerseits gegenüber der Öffentlichkeit, ist jedoch auch angesichts strengerer gesetzlicher Regelungen erforderlich. Führende Branchenakteure wie MOBOTIX nehmen die Problematik ernst und arbeiten aktiv daran, Sicherheit bereits in der frühen Entwicklungsphase in Gerätehardware und -software zu integrieren.

Der Geräteschutz erfüllt jedoch nur dann seinen Zweck, wenn auch für die Sicherheit der gesamten Systemumgebung gesorgt wird. Salopp formuliert: Wer die Tür verriegelt, sollte nicht das Fenster offen lassen. Deshalb müssen Hersteller und Betreiber von Video-Sicherheitssystemen und IoT-Netzwerken das zugrunde liegende Netzwerk, die Speicherinfrastruktur und insbesondere den Faktor Mensch in Betracht ziehen. Letzterer ist häufig das schwächste Glied in der Kette. Branchenverbände wie das SANS-Institut haben diesbezüglich hilfreiche Empfehlungen ausgesprochen. So skizziert beispielsweise das Centre for Internet Security (CIS) in seinen Critical Security Controls konkrete Abwehrmaßnahmen gegen besonders verheerende Formen von Cyberangriffen.[6]

Der Blick in die Zukunft zeigt, dass die Geräte- und Plattformsicherheit für Videotechnologie eine zentrale Rolle spielen wird. Angesichts eines zunehmenden Bewusstseins der Herausforderungen, die mit dem Internet der Dinge verknüpft sind, strebt auch MOBOTIX eine engere Zusammenarbeit mit Branchenakteuren, Kunden und Regierungsbehörden an, um die Technologien und Systeme zu schützen, die unsere Gesellschaft zu einem sichereren Ort machen.

Referenzen

https://www.coresecurity.com/system/files/publications/2016/05/corelabs-ipcams-research-falcon-riva.pdf

https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/

https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf

Quellen

[1]https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.

[2]html https://www.coresecurity.com/advisories/hikvision-ip-cameras-multiple-vulnerabilities

[3]https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/

[4]http://www.telecomtv.com/articles/iot/internet-of-things-to-reach-25-billion-devices-within-five-years-11931/

[5]https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf

[6]https://uk.sans.org/critical-security-controls

Seit 2000 entwickelt und fertigt MOBOTIX IP-Video-Systeme sowie Videoanalyse- und Videomanagement-Software in Deutschland.

MOBOTIX ist für seine außergewöhnlich **hohe Zuverlässigkeit** bekannt. Alle Outdoor-Kameras werden bei Temperaturen von -30 °C bis 60 °C getestet. Sie werden ohne zusätzliche Komponenten, wie Heiz- und Kühlsysteme, und ohne bewegliche Teile (z. B. automatische Blende) bereitgestellt und erfordern praktisch keine Wartung.

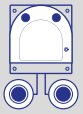
MOBOTIX stellt ein **perfekt durchdachtes Paket** bereit: von der MicroSD-Karte für die Speicherverwaltung über HD-Audio (Mikrofon und Lautsprecher) mit VoIP-Telefonie und Videoanalysen bis hin zu einem professionellen Videomanagement-System und einer Bewegungserkennungssoftware, die für deutlich weniger Fehlalarme sorgt.

Dank der **dezentralen Architektur** ist kein zentraler Computer erforderlich, sodass die Netzwerklast auf ein Minimum reduziert wird. Die intelligenten Kameras von MOBOTIX verarbeiten und speichern Bilddaten automatisch, lösen Ereignisse aus und passen im Fall von Fernzugriff auch Bildrate und Auflösung an die verfügbare Bandbreite an.

Die **6MP-Moonlight-Sensoren** und ergänzende **Wärmebildtechnik** sorgen für eine zuverlässige Detektion von beweglichen Objekten, und zwar auch bei schlechten Lichtverhältnissen und aus weiter Ferne. So können große Bereiche mit nur wenigen Kameras abgesichert werden. Auf diese Weise sinkt der Bedarf an Verkabelung, IT-Infrastruktur oder Zusatzbeleuchtung. Die Kameras von MOBOTIX werden über PoE mit Strom versorgt und erfordern maximal 4–5 Watt.

Mit einem intelligenten IP-Video-System von MOBOTIX können Sie Ihre **Gesamtkosten reduzieren**. Die Investition macht sich schnell bezahlt und ist dank der kostenlosen Software-Updates ausgesprochen zukunftsorientiert.

Outdoor Dual Lens

M16 AllroundDual	S16 FlexMount	D16 DualDome
		
Hohe Zuverlässigkeit auch unter extremen Bedingungen	Flexible Dualkamera	Modulare Dualkamera

Thermal

M16 Thermal	S16 DualThermal
	
Dual-Wärmebildkamera	Dual-Wärmebildkamera

Outdoor Single Lens

M26 Allround	S26 FlexMount	Q26 Hemispheric	D26 Dome
			
Hohe Zuverlässigkeit auch unter extremen Bedingungen	Diskret, Videoanalyse	Diskret, Videoanalyse	Modulare FixDome-Kamera

Indoor

i26 Panorama	c26 Hemispheric	p26 Allround	v26 MiniDome
			
180° hemispheric	Diskret, Videoanalyse	Modulare Decken-Kamera	Vandalismus-Kamera

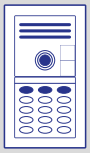
Türmodule

Kamera	BellRFID	Keypad
		

MxDisplay+

Gegenstelle


Tür-Sets

2er-Rahmen		3er-Rahmen	
			

DE_11/17

MOBOTIX AG
Kaiserstraße
D-67722 Langmeil
Tel.: +49 6302 9816-0
Fax: +49 6302 9816-190
vertrieb@mobotix.com
www.mobotix.de

MOBOTIX