FLIR Whitepaper

Konvergenz bei IP-basierten Sicherheitssystemen

Herausforderungen und Lösungen für die Videoüberwachung

FLIR® | The World's Sixth Sense®

Einleitung

Bislang waren die physische Sicherheit und die Netzwerksicherheit zwei grundverschiedene Disziplinen. Die für die Einbruchserkennung, Zugangskontrolle und Videoüberwachung erforderlichen Systeme und ähnlichen physischen Sicherheitstechnologien wurden vorrangig in einer analogen Infrastruktur betrieben; Netzwerke, Server, Computer, Tablets und Smartphones unabhängig davon in einer separaten IP-basierten Infrastruktur. Und als es schließlich zu ersten Überschneidungen zwischen diesen beiden Infrastrukturen kam, stand zunächst die ordnungsgemäße Überwachung und Absicherung des physischen Zugangs zu den Servern und Einrichtungen im Vordergrund.

Heute findet man diese vormals strikte Trennung jedoch immer seltener. Die Kosten-, Flexibilitäts- und Leistungsvorteile, die sich aus der Nutzung einer IP-basierten Infrastruktur ergeben, haben die physische Sicherheit revolutioniert. Nahezu jede Sicherheitskamera- oder Sensortechnologie, die heute auf dem Markt erhältlich ist, lässt sich in einem drahtgebundenen oder drahtlosen Ethernet-basierten Netzwerk nutzen. Dadurch werden physische Sicherheitslösungen wie die Videoüberwachung für dieselben Arten von Angriffen und unbefugten Zugriffen anfällig, unter denen die Datennetzwerke bereits seit Jahrzehnten leiden.

Die Risiken und Vorzüge der IP-basierten Konvergenz werden insbesondere bei Videosystemen deutlich, die in unternehmensweiten Netzwerken betrieben werden. Die hohe Datenübertragungskapazität und geringe Latenzzeit der IP-basierten Infrastruktur bilden in Kombination mit den Kostenvorteilen, die sich aus der Nutzung derselben, ohnehin schon unternehmensweit implementierten Netzwerkinfrastruktur ergeben, die entscheidenden Triebfedern dieser Evolution.

Da die Videoüberwachung heute eine entscheidende Rolle beim Schutz von Einrichtungen, Anlagen und Gebäuden aller Art spielt, die von Eingangsbereichen und Hausfluren über Militärstützpunkte bis hin zu Kraftwerken reichen, hat sich der Schutz der physischen Sicherheitslösung selbst zu einem wichtigen Thema für die Anbieter und Kunden entwickelt. Ältere physische Sicherheitslösungen boten bereits von Haus aus ein gewisses Maß an Sicherheit, da sie nicht mit anderen Systemen verbunden waren. Wollte ein Angreifer ein solches Sicherheitssystem ausschalten oder unbefugt auf das Videoüberwachungsmaterial zugreifen, um dieses zu sichten, zu manipulieren oder zu vernichten, musste er sich am jeweiligen Standort persönlich Zugang zur betreffenden Infrastruktur oder zum betreffenden System verschaffen.

IP-basierte Systeme nutzen hingegen dieselbe Netzwerkinfrastruktur, die bereits im gesamten Unternehmen implementiert ist. Deshalb sind sie wie jedes andere Gerät, das mit dem Internet verbunden ist, auch für dieselben potenziellen Risiken und Bedrohungen anfällig. Komplexe Installationen an mehreren Standorten erhöhen dieses Risiko zusätzlich, da netzwerkfähige Geräte zur Übertragung der Videodaten eine stabile LAN-, WAN- oder Cloud-Verbindung benötigen. Die entsprechenden Überwachungs- und Managementlösungen nutzen in der Regel browserbasierte Anwendungen für den Fernzugriff und die Fernkonfiguration.

Mobile Endgeräte machen diese Herausforderung noch komplexer. Laptops, Tablets und Smartphones, die in ein Videoüberwachungsnetzwerk integriert sind, nutzen Mobilfunkverbindungen für die Netzwerkkommunikation. Diese Netzwerke lassen sich jedoch nicht von den Sicherheitsmanagern überwachen, da ihre Verfügbarkeit und Leistung von externen Drittanbietern abhängt.

Dieses Whitepaper erörtert die sicherheitsrelevanten Herausforderungen bei der IP-basierten Videoüberwachung.

Deshalb müssen die Unternehmen im Rahmen der von ihnen anwendbaren Best-Practice-Methoden sicherstellen können, dass ihre IP-basierten Sicherheitslösungen, die sie zur Absicherung ihrer Netzwerke und Einrichtungen nutzen, ironischerweise nicht selbst zum schwächsten Glied ihrer Sicherheitskette werden.

Die Folgen eines Cyber-Angriffs

Internetkriminelle verfolgen die unterschiedlichsten Ziele. Einige handeln aus politischen Gründen oder weil sie in der weltweiten Online-Community zu zweifelhaftem Ruhm gelangen wollen. Andere attackieren wiederum nur bestimmte Arten von Organisation oder nur solche, die besonders bekannt sind. Ein Cyber-Angriff auf Unternehmensdaten kann schwerwiegende Folgen wie finanzielle Verluste, Diebstahl von Daten, geistigem Eigentum oder vertraulichen Informationen oder ein zerstörtes Kundenvertrauen nach sich ziehen. Ein Angriff, der physische Sicherheitssysteme lahmlegt, kann jedoch neben schweren Sachschäden an der jeweiligen Einrichtung auch zu einer erheblichen Gesundheits- und Lebensgefahr für die davon betroffenen Menschen führen. Daraus können sich wiederum enorme Haftungs- und Schadenersatzansprüche ergeben, die zu tragen eine Organisation am besten gar nicht erst riskieren sollte.

Ein Cyber-Angriff auf Unternehmensdaten kann schwerwiegende Folgen wie finanzielle Verluste, Diebstahl von Daten, geistigem Eigentum oder vertraulichen Informationen oder ein zerstörtes Kundenvertrauen nach sich ziehen.

Wenngleich manche Netzwerkangriffe nur von Einzelpersonen oder Gruppen ausgeführt werden, die lediglich daran interessiert sind, potenzielle Schwachstellen aus reinen Machbarkeitsgründen auszutesten und auszunutzen, geht die größte Gefahr von internationalen Terroristen und Regierungen aus, die professionelle Hacker beschäftigen und jeweils das Ziel verfolgen, kritische Infrastrukturen und physische Sicherheitssysteme gezielt zu zerstören oder lahmzulegen. Diesen Angreifern geht es allein darum, die nationale Sicherheit und die öffentliche Ordnung zu gefährden, um – ohne Rücksicht auf Sachschäden oder menschliche Verluste – ihre eigenen politischen Interessen durchzusetzen, vertrauliche Daten und Informationen zu stehlen oder Rache und Vergeltung zu üben. Ein ähnliches Bedrohungenspotenzial ergibt sich unter anderem durch einheimische Terroristen, organisierte Kriminelle, die sich finanziell bereichern wollen oder unlautere Unternehmen, die Industriespionage betreiben.

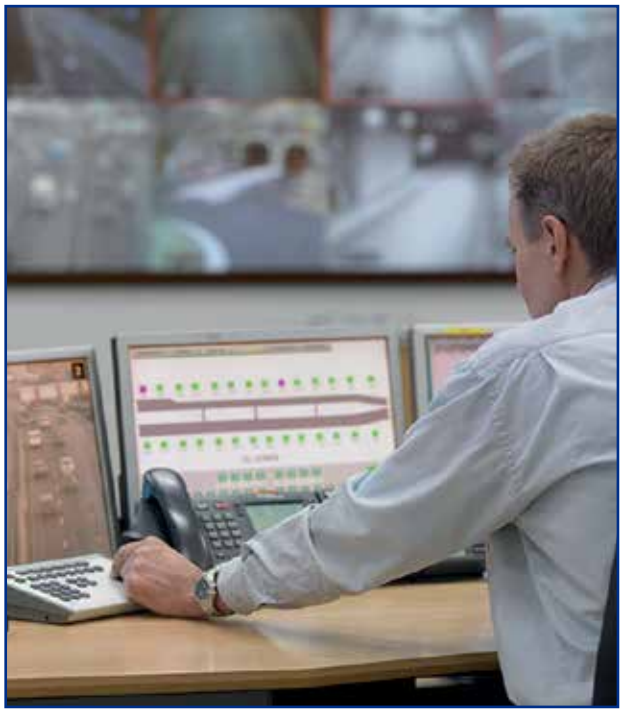
Aber auch interne Bedrohungen stellen stets eine nicht zu unterschätzende Angriffsform dar, die sich leider nur sehr schwer kontrollieren und bekämpfen lässt. Dabei setzen Mitarbeiter oder externe Zulieferer und Dienstleister die Organisation entweder absichtlich oder ungewollt einem entsprechenden Sicherheitsrisiko aus. Die Bedrohungen können dabei von einem absichtlich auf dem Firmenparkplatz platzierten, mit Spyware infizierten USB-Stick über zu schwache Passwörter bis hin zur gezielten Weitergabe von kritischen Informationen oder Zugangsdaten an unbefugte Dritte reichen.

Kurz gesagt: Das Bedrohungs- und Angriffspotenzial im Cyber-Umfeld ist äußerst komplex und kann sich nicht nur von Tag zu Tag, sondern sogar stündlich ändern. Trotzdem sind heute Organisationen aller Größen und die globalen Märkte weltweit miteinander vernetzt. Da der Datenzugriff heute bei Bedarf überall und jederzeit mit jedem Gerät erfolgen kann, ist eine umfassende Sicherheitslösung mit umfassender Bedrohungsabwehr unentbehrlich, um angemessen auf jede erdenkliche Situation reagieren zu können.

Das spezifische Schwachstellenpotenzial der Videoüberwachungssysteme

Videoüberwachungssysteme lassen sich entweder parallel zu anderen IT-Systemen betreiben oder ganz oder teilweise in das Unternehmensnetzwerk integrieren. Dadurch können potenzielle Angreifer die potenziellen Schwachstellen des betreffenden Videoüberwachungssystems gezielt ausnutzen, um entweder das Videoüberwachungssystem selbst anzugreifen oder das zugehörige Netzwerk als

Ausgangspunkt für Angriffe auf andere Systeme innerhalb derselben Organisation zu missbrauchen. Kurz gesagt: IP-basierte Videoüberwachungssysteme unterscheiden sich in diesem Punkt nicht von anderen IT-Systemen. Sie werden in derselben Netzwerk-Infrastruktur betrieben und laufen oftmals auch auf denselben Systemen. Und in den meisten Fällen sind sie ebenfalls permanent mit dem Internet verbunden. Deshalb muss die jeweilige physische Sicherheitslösung auch unbedingt selbst vor IP-basierten Cyber-Angriffen geschützt werden.



Bei einer typischen Implementierung sind die Server und Management-Konsolen mit IP-fähigen Kameras und digitalen Videorekordern (DVRs) verbunden. Diese Systeme interagieren auch mit umfassenderen Sicherheitsmaßnahmen wie Zugangskontrollsystemen oder softwarebasierten Alarm- und Sicherheitsvorfall-Managementlösungen. Dabei entsteht jedoch mit jeder weiteren Netzwerk- oder Querverbindung eine weitere potenzielle Angriffsmöglichkeit für die Cyber-Kriminellen. In diesem Punkt unterscheidet sich ein IP-basiertes physisches Sicherheitssystem also nicht von einer unternehmensbasierten Netzwerksicherheitslösung.

Dennoch unterscheiden sich physische Sicherheits- und Videoüberwachungssysteme durch einzigartige potenzielle Schwachstellen, die alle hinreichend vor möglichen Angreifern geschützt werden müssen. Typische Schwachstellen sind unter anderem:

Speziell entwickelte IP-Geräte

Nahezu jedes IT-System, das aus verschiedenen IP-Endpunkten besteht: Server, Workstations, Switches, Router und mobile Endgeräte. Diese Ausgangssituation stellt jeden IT-Experten hinsichtlich aller Aspekte einschließlich der Abwehr von Cyber-Angriffen vor eine große Herausforderung. Sicherheitsmanagement-Systeme erfordern die Implementierung zusätzlicher IP-Geräte, zu denen unter anderem IP-fähige Kameras, Encoder und Zugangskontrollvorrichtungen gehören. Oft werden diese Geräte jedoch nicht als andere Endpunkte im Netzwerk behandelt. Deshalb macht es für den Angreifer keinen Unterschied, ob er einen CRM-Server, ERP-Server oder eine IP-Kamera angreift, da diese jeweils mit dem Netzwerk verbunden sind und ein Betriebssystem ausführen.

Physisch exponierte Netzwerkkabel und Kameras

IP-Kameras werden überall dort installiert, wo sie gerade gebraucht werden – beispielsweise im Innenbereich einer Organisation, im Perimeter einer Infrastruktur, die komplett ohne Mitarbeiter betrieben wird, oder an öffentlichen Orten wie Parks und Grünanlagen. Dabei sind die Kameras über Ethernet-Kabel mit den Netzwerk-Switches in speziellen Kommunikationsschaltschränken verbunden, die sich oftmals außerhalb eines sicheren Perimeters befinden. Nicht immer ist es generell oder allein schon aus Kostengründen möglich, die zugehörige Infrastruktur komplett abzusichern.

Dann kann ein böswilliger Angreifer einfach die Verbindung zu einer dieser IP-Kameras trennen und anschließend mit seinem Laptop eine Verbindung zum Netzwerk herstellen. Und falls in diesem Netzwerk keine hinreichenden Zugangsberechtigungen und Absicherungsmaßnahmen für die Datenübertragung existieren, wird der Angreifer ab diesem Moment zu einem vollwertigen Bestandteil des gesamten Systems. Er/sie kann dann ungehindert Videomaterial stehlen, Kameras deaktivieren, sich Zugang zu Benutzerdaten verschaffen oder diese manipulieren und andere sensible Daten herunterladen. Außerdem kann der Angreifer diesen Zugang als Ausgangspunkt für Angriffe auf weitere Netzwerke nutzen.

Drahtlose Netzwerke

Noch vor fünf Jahren wurden nur die wenigsten Videoüberwachungssysteme über ein WLAN, Mobilfunk- oder Satellitennetzwerk betrieben. Heute ist dies jedoch bereits

bei fast allen Systemen der Fall, die in der Regel folgende Komponenten, Bereiche und Funktionen umfassen:

- Drahtlose Kameras, die entweder fest installiert sind oder sich bei Bedarf schnell am jeweiligen Standort anbringen lassen
- Tragbare mobile Kameras
- Externe Standorte, die per Satellit eingebunden sind
- Fernzugriff und Fernkonfiguration
- Vermaschte Netzwerke, die in großen Einrichtungen und sogenannten „Safe City"-Implementierungen betrieben werden

Drahtlose Netzwerke sind im jeweiligen geografischen Bereich, den sie abdecken, für jeden Nutzer zugänglich, der über ein geeignetes Endgerät verfügt. Dabei sind die meisten dieser Netzwerke entweder nur unzureichend oder überhaupt nicht verschlüsselt. Wenn diese von externen Dritten wie Mobilfunkanbietern betrieben werden, kann die Organisation deren Sicherheit mangels entsprechender Zugriffs- und Kontrollmöglichkeiten weder überwachen noch gewährleisten. Ohne sorgfältige Konfiguration, Implementierung und Überwachung kann sich durch eine solche – an sich vorteilhafte – drahtlose Zugriffsmöglichkeit ein erhebliches und leider oftmals auch erheblich unterschätztes Sicherheitsrisiko ergeben.

Offene und weitergeleitete Firewall-Ports

Firewalls sind eine grundlegende Technologie, um Unternehmensnetzwerke vor unbefugten Zugriffen zu schützen. Gleichzeitig müssen Firewalls jedoch auch dazu in der Lage sein, erwünschtes Datenaufkommen über spezielle Ports passieren zu lassen, damit eine dauerhaft nutzbare Verbindung zwischen dem Netzwerk und der Außenwelt besteht. Wie bei anderen IT-Systemen erwarten die Anwender auch bei Videoüberwachungsnetzwerken eine Möglichkeit zum Fernzugriff – ganz gleich, ob dieser aus anderen Netzwerken innerhalb derselben Organisation oder von außerhalb der Organisation erfolgt.

Beispielsweise werden einer Unternehmensanwendung wie einem ERP-System dauerhaft der Port 80 oder der Port 443 für andere Niederlassungen und externe Mitarbeiter zugewiesen, damit diese darüber eine Verbindung mit dem zentralen Server herstellen können. Gleichzeitig werden diese Ports aber auch für das sonstige verschlüsselte und unverschlüsselte Online-Datenaufkommen genutzt, das beispielsweise beim reinen Internetsurfen anfällt.

Deshalb können – und sollen – Firewalls das zugehörige Netzwerk niemals komplett von der Außenwelt abschotten. Um das Datenaufkommen und die daraus resultierenden Kapazitätsengpässe beim Ausführen ihrer „normalen" Geschäftsprozesse zu verringern, entscheiden sich einige Organisationen möglicherweise dafür, nicht autorisierte oder untypische Ports zu nutzen, um ihre Kameras, Encoder und DVRs mit ihrem Unternehmensnetzwerk zu verbinden. Dabei wird in einigen Fällen ein Fernzugriff über unzureichend abgesicherte und weitergeleitete Port-Adressen möglich. Wenn das physische Sicherheitspersonal dann nicht über hinreichende Kenntnisse zur Netzwerksicherheit verfügt und die für die Netzwerksicherheit zuständigen Mitarbeiter sich nicht ausreichend mit IP-basierten Videoüberwachungssystemen auskennen, entstehen dabei – wie bereits zuvor erwähnt – ungewollt potenzielle Schwachstellen, die von Angreifern und unbefugten Dritten aufgespürt und ausgenutzt werden können.

Die Herausforderungen der globalen Vernetzung und der „Bring Your Own Device"-Philosophie

Die explosionsartige Ausdehnung von WLAN-, mobilfunk- und satellitengestützten Kommunikationsnetzen hat inzwischen bei den meistern Anwendern die Erwartung geschürt, dass jeder unabhängig von seinem aktuellen Aufenthaltsort jederzeit und mit jedem Gerät auf das Internet zugreifen kann. Und das

trifft natürlich auch auf die Videoüberwachungssysteme zu. Dank Drahtlostechnologie lassen sich Kameras heute auch an abgelegenen und unwegsamen Standorten installieren, an denen eine solche Installation noch vor wenigen Jahren vollkommen undenkbar gewesen wäre. Die Anwender können ihre Geräte einfach per Fernzugriff konfigurieren oder mittels Video-Feeds und Management-Konsolen sowie von Laptops, Tablets und Smartphones jederzeit darauf zugreifen. Für den effektiven Betrieb spielt die Verfügbarkeit eines physischen Anschlusses also heute praktisch keine Rolle mehr.

Gleichzeitig sind diese neuen Zugriffsmethoden aber auch mit neuen sicherheitsrelevanten Herausforderungen verbunden, von denen die meisten bereits zuvor erörtert wurden. Dennoch ergibt sich aus der Möglichkeit zum Fernzugriff auch eine neue Bedrohungsart – die BYOD-Philosophie („Bring Your Own Device"), bei der jeder Nutzer einfach sein persönliches – oftmals privates – mobiles Gerät nutzt. Viele Organisation ermutigen ihre Mitarbeiter dazu, ihre persönlichen Geräte auch für den Zugriff auf Unternehmensressourcen wie Videoüberwachungssysteme zu nutzen. Diese Geräte erfüllen jedoch nur in den seltensten Fällen die Sicherheitsstandards, die sonst im betreffenden Unternehmen für den Malware-Schutz, die Netzwerk-Zugriffskontrolle, Passwörter und sonstigen grundlegenden Sicherheitsmaßnahmen gelten.

Bedenken Sie, was passiert, wenn ein System eine Alarmmeldung ausgibt. Dann müssen sich die Mitarbeiter von zuhause oder unterwegs einloggen, und oftmals haben Sie dafür nur ihr persönliches Smartphone zur Verfügung. Der Druck, einen direkten internen Zugriff auf diese persönlichen Geräte zuzulassen, ist immens, und dieser sollte eigentlich allein schon aus Gründen der Netzwerksicherheit fast immer bis zu einem gewissen Grad von den Nutzern geduldet werden. Denn diese Verbindungen stellen stark frequentierte, aber nur unzureichend geschützte Zugriffswege dar, die sich dadurch gezielt von Angreifern und unbefugten Dritten aufspüren und ausnutzen lassen. Noch schlimmer ist jedoch ein Szenario, bei dem der Angreifer von einem gestohlenen Gerät ohne Passwortschutz oder zu schwachen Passwörtern direkt auf das jeweilige Sicherheitssystem zugreifen kann.

Verlagerung von unternehmensinternen Systemen in die Cloud

Die geringen Kosten und die universelle Verfügbarkeit von cloud-basierten Speicher- und EDV-Systemen betreffen natürlich auch die Videoüberwachungssysteme. In dem Maße, wie das Konzept von eigenständigen physischen und Netzwerk-Perimetern mit der Zeit immer stärker verwischt, entfernt sich auch der Standort, an dem die Videoaufzeichnungen vorgehalten und die zugehörigen Steuerungs-, Kontroll- und Analysefunktionen ausgeführt werden, immer weiter vom eigentlichen physischen Standort.

Gleichzeitig bilden Cloud-Umgebungen ein weiteres Element in der Sicherheitslandschaft, die sich einer Kontrolle durch den Kunden entziehen. Das Sicherheitspersonal muss sich blind darauf verlassen, dass der Cloud-Service-Anbieter ein umfassendes Sicherheits- und Business-Continuity-Programm implementiert hat und dass alle mit der Cloud verbundenen Sensoren und Analysemodule hinreichend vor allen erdenklichen Angriffen geschützt sind.

Ironischerweise lassen sich cloud-basierte Überwachungs- und physische Sicherheitsvorfall-Managementsysteme genauso gut – wenn nicht sogar noch besser – schützen wie unternehmensinterne Systeme. Natürlich werden die meisten Cloud-Anbieter allein schon aus eigenem Interesse alles dafür tun, um die Zuverlässigkeit, Sicherheit und Verfügbarkeit ihrer Systeme zu gewährleisten. Lokalisierte Lösungen lassen sich schlecht implementieren, und oftmals wird den relevanten Sicherheitsbedrohungen dabei nicht genügend Aufmerksamkeit geschenkt.

Das Sicherheitspersonal muss sich blind darauf verlassen, dass der Cloud-Service-Anbieter ein umfassendes Sicherheits- und Business-Continuity-Programm implementiert hat und dass alle mit der Cloud verbundenen Sensoren und Analysemodule hinreichend vor allen erdenklichen Angriffen geschützt sind.

Unabhängig davon, ob eine IP-basierte Videoüberwachungslösung komplett unternehmensintern, in der Cloud oder als Hybridlösung betrieben wird – ohne ein leistungsstarkes und prüffähiges Sicherheitsprogramm sind alle zugehörigen Daten und Services stets für potenzielle Angriffe anfällig. Nutzen mehrere Kunden denselben mandantenfähigen Service und erfolgt die Datenübertragung über öffentliche Netzwerke, kann sich die Situation dadurch zwar weiter verkomplizieren, aber die grundlegenden Probleme bleiben unabhängig vom genutzten Modell immer gleich.

Best Practices für die IP-basierte Videoüberwachung

Obwohl die Risiken für die IP-basierte Videoüberwachung nicht von der Hand zu weisen sind, überwiegen am Ende die Vorteile, die sich aus dem Umstieg von älteren, analog-basierten Systemen auf diese neue Technologie ergeben. Zum Glück können die Videoüberwachungsspezialisten eine wohlverstandene Palette von Best Practices anwenden, mit denen sich physische Sicherheitslösungen hinreichend vor Angriffen und unbefugten Zugriffen schützen lassen.

Bevor wir uns mit den Richtlinien und Methoden befassen, die sich zur Absicherung eines Videoüberwachungssystems eignen, möchten wir Sie noch auf einige wichtige Dinge hinweisen:

- *Es gibt keine Wunderwaffe:*
  Es gibt keine Einzellösung, die komplett vor allen Bedrohungen schützt. Es gibt viele verschiedene Bedrohungen und Angriffsmethoden. Dabei kann ein einzelner Angriff verschiedene Angriffsmethoden umfassen.
- *Eine Kette ist immer nur so stark wie ihr schwächstes Glied:*
  Ein gewiefter Angreifer findet früher oder später immer das schwächste Glied in der Kette, um sein böswilliges Vorhaben auszuführen. Selbst die beste Firewall oder der ausgeklügeltste Verschlüsselungsalgorithmus können am Ende nichts ausrichten, wenn lediglich ein schwaches Passwort wie „1234“ verwendet wird.
- *Jeder ist für die Sicherheit verantwortlich:*
  Und zwar vom Anbieter über den Integrator und Wiederverkäufer (VAR) bis hin zum Endnutzer. Die Anbieter sind offensichtlich für die Entwicklung und Fertigung sicherer Produkte verantwortlich. Dazu gehört unter anderem die Ausführung der zugehörigen Audit-Prozesse und Penetrationstests mittels Software-Code-Analyse und die Konzeption geeigneter Schulungsmaßnahmen für die Integratoren und Wiederverkäufer. Die Integratoren und Wiederverkäufer sind für die Planung einer sicheren Infrastruktur verantwortlich und müssen den Kunden auf alle potenziellen Sicherheitsverstöße und -bedrohungen hinweisen, indem sie die dafür von den Anbietern bereitgestellten Tools und Best Practices nutzen, für ein entsprechendes Anwenderbewusstsein sorgen und die dafür erforderlichen Anwenderschulungen ausführen. Da die Endanwender wahrscheinlich das wichtigste Glied der Kette darstellen, muss man unbedingt dafür sorgen, dass sie nicht gleichzeitig ihr schwächstes Glied sind. Jeder Anwender muss alle potenziellen Bedrohungen kennen und sich stets aller Folgen seines Handelns bewusst sein – und genau dafür muss er hinreichend geschult werden.

Koordination

Die Sicherheit von Videoüberwachungssystemen beginnt mit einer engen Koordination zwischen dem IT- und dem physischen Sicherheitspersonal. Jede dieser beiden Mitarbeitergruppen verfügt über wertvolles Spezialwissen, das die jeweils andere Gruppe benötigt, um insgesamt eine effektive Sicherheit zu gewährleisten. Mitarbeiter, die sich speziell mit Videoüberwachungssystemen auskennen und genau wissen, wie die zugehörigen Kameras, Encoder, Rekorder und Analysemodule mit den Unternehmensnetzwerken

verbunden sind, müssen ihr Wissen an die für die Netzwerksicherheit verantwortlichen Mitarbeiter weitergeben, damit das implementierte physische Sicherheitssystem auch bei der Schwachstellenanalyse und Umsetzung geeigneter Abwehrmaßnahmen (Intrusion Prevention) komplett berücksichtigt werden kann.

Im Gegenzug müssen natürlich auch die für die Netzwerksicherheit verantwortlichen Mitarbeiter alle Infrastruktur-, Zugriffs- und Bandbreitenanforderungen von datenintensiven Prozessen wie der Videoüberwachung genau kennen und verstehen und diese vollständig bei der Erstellung und Umsetzung von umfassenderen unternehmensweiten Sicherheitsprogrammen berücksichtigen. Die Service-Priorisierung, die Netzwerkzuverlässigkeit, der sichere Fernzugriff sowie diverse andere Elemente können sich alle auf die IT-Netzwerk- und sicherheitsrelevanten Prozesse auswirken. Deshalb müssen alle zugehörigen Probleme komplett verstanden, koordiniert und kontrolliert werden, da die physische Sicherheit global in die allgemeinen Netzwerkprozesse integriert ist.

Anbieter-Offenheit

Organisationen, die gerade auf eine IP-basierte Videoüberwachung umsteigen, müssen auf bekannte Schwachstellen in der Firmware und in den Betriebssystemen zugreifen können, die auf bzw. in ihren Kameras, Encodern, Rekordern, Management-Systemen und Analysemodulen ausgeführt werden. Dieses Modell hat sich bereits bestens bei IP-basierten Netzwerkgeräten und Software-Anwendungen bewährt. Deshalb müssen die verantwortlichen Anbieter ihre Videoüberwachungssysteme einschließlich aller zugehörigen Komponenten regelmäßig testen und dabei auch die Rückmeldungen von unabhängigen Testern einbeziehen. Diese Informationen bilden die Vertrauensgrundlage, dass die Produkte hinreichend vor Angriffen geschützt sind und dass Patches und Abhilfemaßnahmen stets rechtzeitig bereitgestellt werden, um die Kundenimplementierungen zu schützen.

Sichere Kommunikationswege

Ein grundlegender Schritt bei der Absicherung von IP-basierten Videoüberwachungssystemen ist offensichtlich ein hinreichender Schutz der Kommunikationswege zwischen den einzelnen Sensoren/Geräten und dem Netzwerk selbst. Zumindest muss die gesamte Datenkommunikation stets komplett verschlüsselt erfolgen Und SSL/TLS muss als Mindeststandard für alle Internetverbindungen genutzt werden, die über einen Webbrowser hergestellt werden.

Virtual Private Networks (VPNs) erhöhen diese Sicherheit zusätzlich. VPNs sind in der Regel nur mit geringen Leistungseinbußen verbunden, sorgen jedoch dafür, dass ausschließlich autorisierte und verschlüsselte Verbindungen genutzt werden – ganz gleich, ob zwischen einer Kamera und dem Netzwerk, zwischen einem externen Anwender und einem DVR oder bei einer beliebigen anderen Verbindungskonstellation innerhalb des gesamten Systems.

Richtlinien für starke Passwörter

Oftmals erweisen sich die verwendeten Passwörter als das schwächste Glied in der gesamten Sicherheitskette. Wenn sie stets ordnungsgemäß umgesetzt werden, können Richtlinien für starke Passwörter die Sicherheit des gesamten Systems jedoch drastisch erhöhen. Die entsprechenden Richtlinien müssen klare Regelungen zu folgenden Punkten enthalten:

- Erforderliche Passwortstärke
- Zeitspanne, nach deren Ablauf ein neues Passwort festgelegt werden muss
- Maximale Anzahl von ungültigen Anmeldeversuchen, nach der das betreffende Benutzerkonto gesperrt wird, um das Erraten von Passwörtern zu verhindern

Zusätzlich sollten Mitarbeiter, die das System per Fernzugriff nutzen wollen, dafür ausschließlich eine Zwei-Faktor-

Ein grundlegender Schritt bei der Absicherung von IP-basierten Videoüberwachungssystemen ist offensichtlich ein hinreichender Schutz der Kommunikationswege zwischen den einzelnen Sensoren/ Geräten und dem Netzwerk selbst.

Authentifizierung (TFA) verwenden. Bei der Zwei-Faktor-Authentifizierung wird für jede Sitzung ein weiteres, zufälliges Passwort oder ein einmaliger zusätzlicher Sicherheitscode generiert. Dadurch wird sichergestellt, dass jeder Anwender einzeln für den von ihm gewünschten Systemzugriff autorisiert wird und dass verlorene oder gestohlene Geräte oder Benutzerdaten keine Sicherheitsbedrohung für das System darstellen. Eine speziell auf die Unternehmensanforderungen zugeschnittene Zwei-Faktor-Authentifizierung validiert alle zugehörigen Anfragen mittels ausgeklügelter Technologien, die sich nur äußerst schwer fälschen oder manipulieren lassen, sowie mittels einzigartiger Codes, die sich von Außenstehenden, die nicht über die dafür erforderlichen internen Spezialkenntnisse verfügen, nicht replizieren lassen.

Netzwerkzugriffskontrolle

Die Netzwerkzugriffskontrolle (NAC) ist eine Sicherheitsmethode, die den Netzwerkzugriff im Einklang mit bestimmten Richtlinien zulässt. Eine der gängigsten NAC-Methoden ist der 802.1X-Standard, bei dem ein Authentifizierungsserver genutzt wird, um jeden Endpunkt zu authentifizieren und zu autorisieren, der versucht, eine Verbindung mit dem Netzwerk herzustellen, bevor ihm der entsprechende Zugriff gewährt wird. Lässt sich ein Endpunkt dabei nicht authentifizieren und autorisieren, wird ihm der Netzwerkzugriff verweigert.

Firewalls

Firewalls bilden nach wie vor das grundlegende Element für den Schutz von Unternehmensnetzwerken. Obwohl sie vorrangig dafür genutzt werden, um eine Organisation vor externen Bedrohungen zu schützen, werden sie auch dafür genutzt, um vertrauenswürdige interne Netzwerke von nicht vertrauenswürdigen internen oder externen Netzwerken zu trennen. IP-basierte Videoüberwachungsnetzwerke werden oftmals mit einer Firewall von anderen Unternehmensnetzwerken getrennt, damit die Risiken, die zur erfolgreichen Ausführung der üblichen Geschäftsprozesse in einem Bereich der Organisation in Kauf genommen werden müssen, nicht das Überwachungssystem gefährden oder im Gegenzug die Risiken, die sich aus der IP-basierten Videoüberwachung ergeben, nicht die Sicherheit der restlichen Netzwerk-Infrastruktur gefährden.

IP/MAC-Filter

Viele IP-Geräte (Router, Switches, Kameras usw.) schränken den Zugriff auf bestimmte IP- und/oder MAC-Adressen ein. Beispielsweise lassen sich Überwachungskameras so konfigurieren, dass sie nur einen Zugriff von einem bestimmten Server zulassen – oder der Server lässt sich so programmieren, dass er nur mit Geräten mit bestimmten, vordefinierten IP- oder MAC-Adressen kommuniziert. Ist ein Gerät nicht in der entsprechenden Whitelist enthalten, wird der Zugriff verweigert. Demzufolge erhält bei diesen Szenario ein Angreifer, der die Netzwerkverbindung einer Kamera im Außenbereich gekapert hat, keinen Zugriff auf das Netzwerk, da sein Computer nicht über die dafür erforderliche korrekte Kennung verfügt.

Physischer Zugriff

Obwohl es im ersten Moment merkwürdig klingen mag, ist die Gewährleistung der physischen Sicherheit einer physischen Sicherheitstechnologie wie beispielsweise einem Videoüberwachungssystem unerlässlich. Jeder direkte Zugriff macht die Geräte und die Netzwerk-Infrastruktur für potenzielle Angriffe und unbefugte Zugriffe anfällig. Da von den Kameras bis zu den Serverschränken jede Netzwerkkomponente hinreichend vor nicht autorisierten physischen Zugriffen geschützt werden muss, unterscheiden diese sich nicht von anderen wertvollen Unternehmensressourcen. Demzufolge muss jeder persönliche Zugriff auf jeglichen Bestandteil des Videoüberwachungssystems streng auf die dafür autorisierten Mitarbeiter beschränkt werden.

Angriffserkennung und -vermeidung

Die vorgenannten Vorschläge konzentrieren sich vorrangig auf die Vermeidung von Angriffen, Bedrohungen und unbefugten Zugriffen. Andere Tools und Prozesse, die vorwiegend aus den Netzwerksicherheitssektor stammen, ergänzen diese Empfehlungen mit einer Funktion, mit der sich die Infrastruktur auf Schwachstellen überprüfen lässt, um unzulässige oder nicht autorisierte Netzwerkzugriffe oder -aktivitäten sowie laufende Angriffe zu erkennen und zu stoppen. Obwohl sich diese Technologien insbesondere bei umfangreichen Implementierungen oftmals nur relativ umständlich für die jeweiligen unternehmensspezifischen Videoüberwachungsanforderungen konfigurieren lassen, erweisen sie sich beim Schutz von stark gefährdeten Installation als äußerst wirksam.

Fazit

Zur Umsetzung eines effektiven Sicherheitsprogramms müssen nicht nur alle internen Organisationsebenen, sondern auch alle externen Anbieter, Integratoren, Wiederverkäufer und Anwender mit Fernzugriffsmöglichkeit ihren Beitrag leisten. Dabei gilt es jedoch unterschiedliche Sicherheitsformen zu beachten. So können beispielsweise für die IP-basierte physische Sicherheit und für die Netzwerksicherheit – obwohl beide Formen dieselben Tools und dieselbe Infrastruktur nutzen – unterschiedliche Richtlinien und Verfahrensweisen für die Umsetzung eines effektiven Sicherheitsprogramms gelten. Deshalb ist es unerlässlich, dass das physische Sicherheitspersonal und die für die Netzwerksicherheit zuständigen Mitarbeiter stets eng zusammenarbeiten und die einzigartigen Missionskriterien der jeweils anderen Gruppe vollständig verstanden haben.

Auch die Anbieter, Integratoren und Wiederverkäufer spielen dabei eine wichtige Rolle, denn diese externen Dritten stehen für ein breites Spektrum von Sicherheitsprodukten, -infrastrukturen und -implementierungen. Sie werden durch ihre tägliche Arbeit mit weitaus mehr Schwachstellen und Sicherheitsverstößen konfrontiert als die Endnutzerorganisationen und können ihren Kunden durch ihr dabei gesammeltes Spezialwissen helfen, genau die Tools und Prozesse auszuwählen, die sich am besten für den Schutz ihres Unternehmens eignen. Außerdem können sie für ein entsprechendes Anwenderbewusstsein sorgen und die dafür erforderlichen Anwenderschulungen ausführen. Dabei ist das letzte Element für den Erfolg des jeweiligen Sicherheitsprogramms entscheidend, da die Endanwender häufig das schwächste Glied der gesamten Sicherheitskette darstellen und sich gleichzeitig am schwierigsten beeinflussen lassen.

Deshalb sind die Anbieter von IP-basierten Videoüberwachungssystemen wie FLIR auch dafür verantwortlich, das Überwachungssystem selbst hinreichend vor Angriffen und unbefugten Zugriffen zu schützen. Dafür sieht die FLIR IP-mmune-Plattform, die unter dem Namen ASIS 2015 auf dem Markt eingeführt wurde, eine Reihe von Angeboten vor, die sich innerhalb eines sicherheitsspezifischen Rahmenwerks betreiben lassen. Einige dieser Elemente sind auch als einzelne Produkte und Services erhältlich. Andere sind wiederum ein fester Bestandteil jedes FLIR IP-basierten Produkts, beispielsweise die Verschlüsselung und Serverabsicherung innerhalb der FLIR Video-Managementsystem-Anwendungsreihe (VMS). Außerdem arbeitet FLIR eng mit den zuständigen Zertifizierungs- und Regulierungsbehörden wie dem National Institute of Standards and Technology (NIST) zusammen, um sicherzustellen, dass alle FLIR-Produkte stets alle aktuellen und zukünftigen Standards für einen sicheren Betrieb erfüllen.

Die IP-basierte Videoüberwachung ist eine leistungsstarke und kostengünstige Plattform, mit der sich die Reichweite, Flexibilität, der Nutzwert und die Finanzierbarkeit dieser kritischen physischen Sicherheitslösung deutlich verbessern

Die IP-basierte Videoüberwachung ist eine leistungsstarke und kostengünstige Plattform, mit der sich die Reichweite, Flexibilität, der Nutzwert und die Finanzierbarkeit dieser kritischen physischen Sicherheitslösung deutlich verbessern lässt.

lässt. Die größte Herausforderung besteht darin, dass die Infrastruktur selbst vor netzwerkbasierten Angriffen und unbefugten Zugriffen geschützt werden muss. Zum Glück sind dafür bereits alle erforderlichen Tools, Schulungsmaßnahmen und operativen Prozesse verfügbar. Mit einem sorgfältig geplanten und implementierten Sicherheitsprogramm können Unternehmensorganisationen einen vertrauensvollen Umstieg von analogen auf digitale Videoüberwachungssysteme vollziehen, da sie sich stets beruhigt darauf verlassen können, dass alle potenziellen Schwachstellen bereits beim Anbieter bekannt sind und kontinuierlich von ihm überwacht und berücksichtigt werden.

Um weitere Informationen zur IP-basierten Videoüberwachung, Netzwerksicherheit für IP-basiere physische Sicherheitslösungen und den FLIR-Produkten und -Services zu erhalten, wenden Sie sich bitte an eine unserer unten stehenden Niederlassungen oder senden Sie uns eine E-Mail an flir@flir.com.

Über FLIR Systems

FLIR Systems, Inc. ist weltweiter Marktführer im Bereich Entwicklung, Herstellung und Vertrieb von Sensorsystemen, die die Wahrnehmung und das Bewusstsein stärken. Die fortschrittlichen Systeme von FLIR werden für eine Vielzahl unterschiedlicher Wärmebild-, Situationsbewusstseins- und Sicherheitsanwendungen eingesetzt, unter anderem in den Bereichen luft- und bodengestützte Überwachung, Zustandsüberwachung, Navigation, Freizeit, Forschung und Entwicklung, Herstellungsprozesskontrolle, Suche und Rettung, Drogenbekämpfung, Transportsicherheit, Grenz- und Wasserpatrouille, Umweltüberwachung sowie Erkennung von Bedrohungen durch chemische, biologische, radiologische, nukleare und explosionsgefährdete Stoffe (CBRNE). Weitere Informationen finden Sie auf der FLIR-Website unter www.FLIR.com.

Die Bilder dienen nur zur Veranschaulichung. ©2016 – FLIR Systems Inc., Alle Rechte vorbehalten (erstellt 02/16)

FLIR Portland
Corporate Headquarters
Flir Systems, Inc.
27700 SW Parkway Ave.
Wilsonville, OR 97070
USA
PH: +1 886.477.3687

FLIR Commercial Systems
Luxemburgstraat 2
2321 Meer
Belgium
Tel. : +32 (0) 3665 5100
Fax : +32 (0) 3303 5624
E-mail : flir@flir.com

FLIR Systems GmbH
Berner Strasse 81
D-60437 Frankfurt am Main
Germany
Tel. : +49 (0)69 95 00 900
Fax : +49 (0)69 95 00 9040
E-mail : flir@flir.com

www.flir.com
NASDAQ: FLIR