IT-Risiken bei Netzwerk Videoüberwachung

Kamera-Anbieter denken bisher kaum an die Gefährdung

Wer heute in moderne Überwachungstechnik investieren möchte, erhält ein riesiges Angebot an IP-basierten Kamerasystemen. Die starke Reduktion der Gesamtkosten für die Videoüberwachung ist neben der Flexibilität der entscheidende Treiber dieser Technologie. Die offensichtlichen Vorteile dürfen aber nicht zu Lasten der Sicherheit gehen. Um mit dieser Infrastruktur eine sichere und manipulationsresistente Überwachung zu gewährleisten, sind bestimmte Vorkehrungen zu treffen, die von den Herstellern nicht immer in den Vordergrund gestellt und teilweise auch nicht angeboten werden.

Von Prof. Dr. Norbert Pohlmann, Marco Smiatek und Sebastian Spooren, Gelsenkirchen

Die Vorteile der IP-basierten Kamerasysteme liegen auf der Hand. Im Gegensatz zur klassischen BNC-Technologie, die für jede Kamera eine spezielle Verkabelung benötigt, benutzen neue Modelle die zumeist vorhandene TCP/IP Netzwerk Infrastruktur. Bei Neuinstallationen entfällt das aufwändige Verlegen von Kabeln bis zur Zentrale, Aufnahmegeräte wie Videorecorder und Überwachungsmonitore werden durch herkömmliche PC ersetzt und die passende Software liefert der Hersteller der Kamera gleich mit. Die Konfiguration der Systeme erfolgt via Webbrowser, zusätzliche Kabel zur Stromversorgung sind für die Kameras häufig nicht mehr erforderlich, da fast alle IP-basierten Kamerasysteme heute per „Power over Ethernet" angeboten werden.

IP-basierte Kamerasysteme können über das lokale Netzwerk hinaus per Internet erreichbar gemacht werden. Besteht eine ausreichend schnelle Anbindung an das weltumspannende Datennetz, können die aktuellen Videostreams der verschiedenen Netzwerkkameras nahezu in Echtzeit an jeden Ort der Welt übertragen werden. Allerdings birgt diese Möglichkeit auch eine Erhöhung des Gefahrenpotenzials, da theoretisch jede Personen weltweit Zugriff auf die Kameras bekommen könnte, sofern die Geräte nicht ausreichend abgesichert sind. Beispiele für ungeschützte Kameras lassen sich einfach per Google finden. Suchbegriffe wie „google hacking kamera" führen zu Kameras, die zum Beispiel Hinterhöfe, Parkplätze und Unternehmensräume überall auf der Welt zeigen – sichtbar für jeden! Die Zoom-Einstellungen und auch die Bewegungen der Kameras lassen sich dabei direkt steuern. Sowohl datenschutzrechtlich als auch sicherheitstechnisch sollten viele dieser Kameras sicherlich nicht von jedem Online-Nutzer gefunden und bedient, sowie der Videostream eingesehen, werden können. Es gibt sogar zahlreiche Bücher zu diesem Thema im Rahmen des so genannten „Google Hacking". Dieselbe Problematik gilt übrigens für alle IP-gestützten Systeme, wie beispielsweise auch Drucker.

Werksseitig werden bei den IP-Geräten meist keine Sicherheitsfeatures aktiviert, auch wenn sie verfügbar sind. Ein Installateur ohne detaillierte Netzwerkkenntnisse findet meist keine oder nur unzureichende Hinweise vom Hersteller, wie er ein solches System ausreichend vor Angriffen schützen kann. Was gilt es zu beachten?

Https – das „s" ist entscheidend!

Die IP-basierten Kamerasysteme werden – in Analogie zu modernen Druckern oder Routern – über einen handelsüblichen Browser wie Mozilla Firefox oder Microsoft Internet Explorer konfiguriert. Das Konfigurationsmenü ist über eine Weboberfläche erreichbar, die über den Browser aufgerufen wird. Die Kameras stellen diese Funktion über einen integrierten Webserver bereit. Über die Konfigurationsoberfläche wird eine Anmeldung (Authentifizierung) meist per Benutzername und Passwort verlangt, um Einstellungen ändern zu können. Der komfortable Einsatz ohne Extra-Installation eines Konfigurationsprogramms bietet große Vorteile für die Nutzer, aber auch eine Chance für Angreifer. Die Webserver auf den Kameras sind gemäß der Werkseinstellung immer unverschlüsselt via http zu erreichen. Ein Angreifer wird dadurch in die Lage versetzt, die komplette Kommunikation zwischen Kamera und Benutzer mitzulesen und damit in den Besitz von schützenswerten Zugangsdaten wie Benutzername und Passwort zu kommen. Dabei lässt sich dieses Problem bei einigen Produkten mit einem einfachen Haken in der Konfigurationsmaske lösen. Er sorgt dafür, dass eine Kommunikation nur verschlüsselt per https zugelassen wird. Https nutzt das vom Online-Banking bekannte SSL-Protokoll. Auch hier lauern Stolpersteine: Es ist natürlich anzuraten, zuerst die verschlüsselte Kommunikation per https zu aktivieren und erst danach das Passwort zu ändern und die Einstellungen zu tätigen.

Einen Hinweis, wie man die Geräte si-

cher konfiguriert, sucht man in den QuickSetup Guides vieler Hersteller allerdings vergebens. Nur wer weiß, wonach er suchen muss, wird im ausführlichen Handbuch fündig. Wünschenswert wäre hier eine Checkliste zur sicheren Konfiguration vom Hersteller im QuickSetup Guide oder als Beilage. Noch besser wäre es, die Werkseinstellungen auf die genannten Sicherheitsbedürfnisse hin anzupassen.

Sichere Passwörter

Wird die Kamera in ein Netzwerk integriert, kann über einen Browser das Konfigurationsmenü aufgerufen werden. Der Zugriff ist werksseitig mit einem Standardpasswort geschützt. Bei den meisten Produkten zwingt das Konfigurationsprogramm den Benutzer jedoch nicht, das Passwort zu ändern. Wird man gezwungen es zu ändern und es weicht daraufhin nicht vom alten Passwort ab, wird in der Regel kein Hinweis auf eine damit einhergehende Sicherheitslücke gegeben. Ein potenzieller Angreifer findet das Standardpasswort im Regelfall auf den Webseiten des Herstellers in Form einer Bedienungsanleitung, die zum Download bereitsteht. Damit kann er sich sehr schnell und einfach Zugang zum Kamerasystem verschaffen. Hier ist der Installateur gefordert, ein sicheres Passwort zu wählen. Im Idealfall sollte die Kamerasoftware den Benutzer zwingen, das Passwort nach der ersten Anmeldung zu ändern. Dabei muss die Software die erneute Vergabe des Ursprungspassworts verhindern und das neue Passwort auf Komplexität im Bezug auf Länge und Zusammensetzung (Zahlen, Buchstaben, Sonderzeichen) prüfen.

Weitere Gefahren bei Wireless LAN

Die neue Generation Kameras nutzt Ethernet-Computernetzwerke und bietet dadurch auch die Verwendung von Wireless LAN (kurz: WLAN). Daraus ergibt sich der Vorteil, dass die Kameras an nahezu jedem Ort platziert werden können, auch dort wo der Einsatz über Netzwerkkabel nur schwer möglich wäre oder eine Verkabelung nicht vorhanden ist. Der Nachteil hierbei ist, dass die Funkverbindung neben den Vorteilen auch weitere Risiken mit sich bringt, wenn die Konfiguration nachlässig gestaltet wird – denn nicht jede WLAN-Verschlüsselung ist sicher (unsicher: WEP-Verschlüsselung). Um eine ausreichende Verschlüsselung zu gewährleisten, sollte in jedem Fall WPA2 eingesetzt werden, da für WPA TKIP Anfang November 2008 eine erste Schachstelle gefunden wurde. Hierbei ist es wichtig, dass bei der Verwendung von „WPA2 Personal“ für die Verschlüsselung ein starkes Passwort gewählt wird.

WLAN Kameras lassen sich recht leicht an ihrer Antenne erkennen. Potenzielle Angreifer könnten dieses Wissen ausnutzen und die Kommunikation mit der per Funk angebundenen Kamera jederzeit mit einem Störsender unterbrechen, wenn es ihren kriminellen Zwecken dient. Der Erfolg des Angriffs relativiert sich jedoch, wenn die Kamera alle Bilder, auch intern, zum Beispiel auf eine Speicherkarte für eine spätere Auswertung sichert.

Verschlüsselung des Videostreams

Kameraüberwachung ist normalerweise in sicherheitskritischen Bereichen im Einsatz. Ein Ausfall der Kamera oder das Senden falscher Bilder durch Einspielungen, wie es aus Kriminalfilmen bekannt ist, könnte verheerende Folgen haben. Die Verfügbarkeit, die Integrität und Authentizität sind damit die entscheidenden Parameter bei der Übertragung von Bildern. Die meisten Kamerasysteme benutzen zur Übertragung des Bildes das so genannte Real Time Streaming Protokoll (RTSP). Ohne Verschlüsselung des Streams bekommt jeder, der Zugriff auf das Netzwerk hat, die Möglichkeit, den Videostream zu verfolgen, der eigentlich nur dem Sicherheitsdienst oder autorisierten Personen vorbehalten sein sollte. Bei IP-basierten Systemen können das sehr viele Personen sein, wie im Google Hacking Beispiel bereits aufgezeigt wurde. Ein mögliches Angriffsszenario wäre ein Denial of Service (DoS) Angriff, bei dem die Kamera mit so vielen Anfragen überfordert wird, dass sie zunächst aufgrund der Überlastung nicht mehr erreichbar ist. Ein Angreifer kann daraufhin eine entsprechend manipulierte Szene in das Netzwerk einspeisen, die scheinbar von der Kamera übertragen wird. Da bislang kein verschlüsseltes Streaming-Protokoll existiert, ist hier die Initiative der Hersteller gefordert, ein solches zu entwickeln oder ihre Produkte um Verschlüsselungshardware und -software zu erweitern. Der Einsatz ▶

Tipps für den sicheren Einsatz von Netzwerkkameras

- ***Konfiguration immer über gesicherte Verbindung abwickeln!***
  Achten Sie darauf, dass bei der Konfiguration das Protokoll „https“ und nicht „http“ verwendet wird (SSL/TLS-Verschlüsselung).
- ***Standardpasswort des Konfigurationsprogramms ändern!***
  Sie sollten in jedem Fall das Standardpasswort vom Konfigurationsprogramm ändern. Verwenden Sie hierzu ein sicheres Passwort, das mindestens zehn Stellen besitzt und möglichst aus Zahlen, Buchstaben und Sonderzeichen sinnfrei zusammengesetzt ist.
- ***Benutzerkonten anlegen!***
  Für Personen, die ausschließlich den Videostream der Kamera einsehen dürfen, sollten Benutzerkonten mit nur dafür notwendigen Rechten angelegt werden. Verwenden Sie hierfür niemals das Admin-Benutzerkonto.
- ***Signieren und verschlüsseln!***
  Wenn Sie hohe Sicherheit benötigen, achten Sie darauf, dass die Kamera den Stream bzw. die Bilder zumindest signiert, um eine Manipulation der Daten auszuschließen. Fragen Sie bei Ihrem Hersteller, ob eine Verschlüsselungsmöglichkeit in Zukunft nachgerüstet werden kann. Achten Sie darauf, dass die Signatur/Verschlüsselung direkt auf der Kamera durchgeführt wird.
- ***WPA2 als WLAN-Verschlüsselung verwenden!***
  Es sollte kein Zertifikat sondern ein sehr komplexes Passwort verwendet werden. Zu empfehlen ist, die hier möglichen 63 Zeichen mit Groß- und Kleinbuchstaben sowie Sonderzeichen und Zahlen vollständig auszuznutzen.
- ***Kamera mit internem Speicher vorteilhaft!***
  Besonders bei Funkverbindungen ist es günstig, wenn die Kamera über einen internen Speicher verfügt, auf dem die Aufzeichnung gespeichert wird. Damit gehen auch bei Netzausfällen keine Daten verloren.

Sichere Netzwerkkameras

Anbieter	AASSET Security GmbH	Axis Communications GmbH	Bosch Sicherheitssysteme GmbH
Welche Sicherheitsfeatures sind in Ihren Netzwerkkameras vorhanden/möglich?			
Zugriffsschutz durch Passwort?	in allen Modellen	in allen Modellen	in allen Modellen
Sichere Übertragung durch SSL-Verschlüsselung?	nein	in allen Modellen	in allen Modellen
Verschlüsselung v. Einzelbild/Stream i. d. Kamera?	nein	in allen Modellen	in allen Modellen
Ist eine Firewall in der Kamera integriert?	nein	nein	nein
Welche Verschlüsselungsprotokolle bieten Sie für WLAN-Lösungen an?	keine Modelle	WEP40, WEP128, WPA-PSK, WPA-Enterprise, WPA2-PSK und WPA-Enterprise	keine Modelle
Beispiel für Kamera/Kamera-Familie mit hohem Sicherheitsanspruch	**SNC-B2315P / SNC-B5395P / SNC-M300 von Samsung Electronics**	**AXIS 211W**	**Dinion XF IP, FlexiDome XF IP. AutoDome IP**
Zugriffschutz für die Kamera			
Ist ein Standard-Passwort gesetzt?	ja	nein	nein
Wird der Benutzer bei der Erstnutzung gezwungen ein eigenes Passwort zu erstellen?	nein	ja	nein
Wird das Passwort bei Neueingabe auf Sicherheit geprüft?	nein	nein	nein
Können im Umfang unterschiedliche Zugriffsrechte auf der Kamera realisiert werden?	ja, über Softwareeinstellungen	ja, in 3 Benutzerebenen	ja
Welche weiteren Maßnahmen, zur Verhinderung von Angriffen über das Netz werden eingesetzt?	nein	IP-Filter können genutzt werden	Einstellung der gewünschten Ports
Was passiert, wenn per NTP ein falsches Datum/Uhrzeit übergeben wird?	wird übernommen	k.A.	NTP ist der maßgebende Zeitgeber
Gibt es darüber hinaus besondere Sicherheitsmaßnahmen für Firmware-Updates bzw. zur Verhinderung von Manipulationen an der Kamerasoftware?	nur Admin kann Firmware-Updates einspielen	nein	Passwortschutz
Werden alle Zugriffe /Zugriffsversuche in der Kamera protokolliert?	ja	ja	ja
Zugriffsschutz bei der Datenübertragung			
Ist eine SSL-Übertragung möglich?	nein	ja	ja
Ist die SSL-Übertragung als Standard voreingestellt?	–	nein	nein
Kann ein eigenes SSL-Zertifikat hochgeladen werden?	–	ja	ja
Wird eine PKI unterstützt?	nein	nein	nein
Können Bilder/Streams vor der Übertragung (kryptologisch) verschlüsselt werden?	nein	nein	ja, per AES
Können Bilder/Streams vor der Übertragung signiert (gegen Veränderung geschützt) werden?	nein	nein	nein
Ist das Thema Informationssicherheit Gegenstand der Schulung Ihrer Errichterpartner?	ja	ja	ja
Wird die Firmware der Kamera bzw. die Software zur Datenübertragung regelmäßig auf Sicherheitslücken geprüft?	ja	ja	ja
Erhält der Anwender in der Benutzeranleitung ausführliche Sicherheitshinweise?	nein	ja	ja
Web-Adresse	www.aasset.de	www.axis.com	www.bosch-sicherheitsprodukte.de

Sichere Netzwerkkameras

... sind nur für wenige Hersteller bisher ein relevantes Thema. Anfang November hatten wir fast 60 in Deutschland tätige Anbieter von IP-Kameras angeschrieben, sieben von diesen haben geantwortet. Üblich waren bei Marktübersichten im Videobereich bisher Rücklaufquoten von über 70%. Offensichtlich denken aber auch Kunden und Errichter nicht daran, dass Netzwerkkameras Kleincomputer mit Objektiv sind und damit ebenso den Gefährdungen der IT ausgesetzt sind wie alle anderen Geräte in IT-Netzen. So wurde sowohl bei unserer Marktbefragung wie auch auf der Messe SECURITY deutlich, dass sich bei vielen Anbietern weder Vertrieb noch Produktmanager sich bisher mit diesen Fragen befassen mussten.

bereits etablierter Techniken wie SSL-Tunnel oder einem Virtual Private Network (kurz: VPN) wäre hier schon ein enormer Fortschritt, da damit sichergestellt würde, dass kein Unbefugter die Bilder einsehen könnte.

Im Idealfall wird der Datenstrom digital signiert und verschlüsselt, um Vertraulichkeit, Authentizität, Integrität und Verbindlichkeit der Daten zu gewährleisten. Erste Ansätze sind bei einigen Herstellern bereits zu erkennen, so verwendet ein Unternehmen zum Beispiel kein Streaming, um die Bilder zu übertragen, sondern kopiert Bild für Bild über das Netzwerk. Jedes Bild wird mit einer Signatur versehen, aus der unter anderem zu erkennen ist, welche Kamera zu welchem Zeitpunkt ein Bild erstellt hat. Diese gültige Signatur sagt auch aus, dass das Bild in keiner Weise manipuliert wurde.

Fazit:
Jeder der IP-basierte Kamerasysteme einsetzt, muss sich darüber bewusst sein, dass diese werksseitig mit den

Die Angaben der Marktübersicht beruhen auf Angaben der Anbieter und wurden von der Redaktion nicht auf sachliche Richtigkeit geprüft. Stand der Marktübersicht: 25.9.2008

	Funkwerk plettac electronic GmbH	MOBOTIX AG	Pelco Germany	Siemens BT – Fire Safety & Security Products GmbH & Co. oHG
	in allen Modellen	in allen Modellen	in allen Modellen	in allen Modellen
	nein	in allen Modellen	nein	nein
	nein	in allen Modellen	teilweise	teilweise, HTTP(S)
	nein	nein	nein	in allen Modellen
	keine Modelle	keine Modelle	Pelco Security Protokoll oder erweitertes WPA/PSK	WEP, WPA-PSK und WPA2
	FAC 9400 IP	**MOBOTIX M12, D12, M22, D22, Q22, V12, DevKit**	**Spectea VI IP, Spectra Mini IP, IP110 im Endurabetrieb**	**CCIx1345 (CCIC1345, CCIS1345 u. CCIW1345) Farb-, Tag/Nacht-, und Wide-Dynamic-Modell**
	ja	ja	ja	ja
	nein	ja	nein	nein
	nein	nein	nein	nein
	nein	ja, umfangreiches Benutzer-/Gruppenmanagement mittels Rechtevergabe: Ansicht, Zugriff aus dem Managementsystem, Parametrierung und Ereigniseinstellungen können benutzer-/gruppenspezifisch freigegeben werden. Darüber hinaus kann eine zeitliche Zugriffsbeschränkung erfolgen.	ja unterschiedliche Gruppen	ja, Administrator und unterschiedliche Benutzerrechte. Admin: voller Zugriff, Advanced User: Bedienung u. S/N-Steuerung, Einfacher Nutzer: Videobildabruf
	keine	IP-Filter, Intrusion Detection, Digital Signatures Fingerprint (Header des Bildmaterials), RADIUS (IEEE 802.1X)	keine	Integrierte Firewall mit IP-Filtering, Port- und Protokoll-Sperre, HTTP(S)
	wird ignoriert, System läuft auf interner Uhr, übergeordnete Synchronis. d. Managementsystem P.O.S.A.	k.A.	k.A.	keine Auswirkung
	ja, Sperre von Web-Server und FTP-Protokoll ist per serieller Schnittstelle möglich und kann auch nur dadurch wieder aufgehoben werden	Firmware ist verschlüsselt, Kamera nimmt nur Firmware mit spezieller MOBOTIX-Signatur an (symmetrisches Verschlüsselungsverfahren), Firmware wird durch Checksum geprüft	nein	Firware-Updates nur über Administrator-Rechte durchführbar
	ja (Signalisierung an Managementsystem durch SNMP-Trap und proprietärem Steuerungsprotokoll)	ja (Webserver-Logdatei mit 2048 Einträgen, Mehrfachzugriffe von derselben IP-Adresse werden samt Zeitstempel in ein einzigen Eintrag gebündelt)	ja	ja (bei mehrfach fehlerhaftem Zugriffsversuch erfolgt Alarmmeldung z.B. per e-Mail, Protokollspeicher kameraabhängig (max. 32 kB))
	nein	ja	nein, aber eigener Standard	nein
	–	ja	–	–
	–	ja	–	–
	nein	ja	ja	nein
	nein	nein	ja, per AES128	nein
	nein	ja (Digitale Signierung via X.509 Zertifikat)	ja	nein
	ja	ja	ja	ja
	ja	ja	nicht bekannt	ja
	ja	ja	nein	ja
	www.plettac-electronics.de	www.mobotix.com	www.pelco.com	www.siemens.com/cctv www.siemens.de/fsp

niedrigsten Sicherheitseinstellungen ausgeliefert werden. Es liegt also beim Installateur, die SSL-Verschlüsselung (https) zu aktivieren, ein sicheres Passwort zu setzen und die Kamera optimal zu konfigurieren. Einige Anbieter verzichten außerdem auf diverse Sicherheitsfunktionen, die für den vertrauenswürdigen Einsatz notwendig sind. Die Technologien sind vorhanden, es geht nur darum, die Hersteller zu veranlassen, diese zu implementieren und auch werksseitig zu aktivieren bzw. in den Vordergrund zu stellen. Erst wenn von vielen Kunden der Bedarf an Sicherheit zu den Herstellern getragen wird, werden diese ihre Sicherheitstechnik auch weiter verbessern, denn das übertragene Bild kann zurzeit in den meisten Fällen noch von jedem im Netzwerk eingesehen werden.

Über unsere Autoren:

Prof. Dr. Norbert Pohlmann ist geschäftsführender Direktor des Instituts für Internet-Sicherheit if(is) an der Fachhochschule Gelsenkirchen.
Marco Smiatek ist Student der angewandten Informatik der Fachhochschule Gelsenkirchen und studentischer Mitarbeiter am if(is). Seine Aufgaben umfassen die Erstellung von Live-Hacking-Szenarien und die Forschung und Entwicklung im Bereich Trusted Computing.
Sebastian Spooren, Dipl.-Informatiker (FH), ist wissenschaftlicher Mitarbeiter am if(is), Projektleiter vom Branchenbuch IT-Sicherheit und u.a. mit der Darstellung von Gefahren und Risiken für die Öffentlichkeit und der Forschung und Entwicklung im Bereich Scientific Visualization, um den Zustand des Internets abzubilden, befasst.
Kontakt: www.internet-sicherheit.de