Cyber Security und Cloud Videoüberwachung

In diesem Dokument wird erklärt, warum und wie die Sicherheit von Videoüberwachungssystemen in der Branche umfassender behandelt werden kann und sollte, damit die Cyber-Sicherheit kein Problem für Installateure oder Kunden mehr darstellt. Eagle Eye Networks ist in dieser Hinsicht Marktführer und mindert Sicherheitsbedenken hinsichtlich Produktforschung, -entwicklung und -einsatz.

Introduction

Figure 1. Timeline: escalating cyber attacks on security video cameras and DVRs.

Die heutigen vernetzten Videoüberwachungssysteme sind in vielerlei Hinsicht anfällig, und ihre Kameras wurden von Hackern mit Waffen versehen, um massive DDoS-Angriffe (Distributed Denial of Service) auf Zielsysteme zu erzeugen. Die Abbildung 1 zeigt eine Zeitleiste der jüngsten Cyber-Angriffe und Bedrohungen, die mit Internet verbundene Überwachungskameras und digitale Videorecorder (DVRs) betreffen.

Die Sicherung der heutigen vernetzten Videosysteme kann eine komplexe und schwierige technische Herausforderung sein. Gerade für kleine und mittelständische Unternehmen muss es jedoch nicht so sein. Videosysteme und -ausrüstungen können im Gegensatz zu der derzeitigen installierten Basis der vernetzten Videotechnologie zweckbestimmt sein, um ein vorgeschütztes und leichter zu sicherndes System zu bilden.

Im September 2016 meldete ein großer französischer Webhosting-Anbieter eine rekordverdächtige DDoS-Attacke von 1 Terabit pro Sekunde auf seine Webserver, ausgelöst durch eine Sammlung von mehr als 145.000 gehackten Internet-verbundenen Videokameras und digitalen Videorekordern.

Im Oktober 2016 wurden DDoS-Angriffe von mehreren zehn Millionen IP-Adressen gegen Dyn, ein Internet-Infrastrukturunternehmen mit Hauptsitz in New Hampshire, gestartet. Die Attacken haben Dutzende von großen Websites wie AirBnB, Amazon, Etsy, GitHub, Netflix, Pinterest, Reddit, PlayStation Network, SoundCloud, Spotify und Twitter lahm gelegt oder offline gestellt.

Forscher haben berichtet, dass über 90% der angegriffenen Geräte kompromittierte Netzwerk-Überwachungskameras und DVRs waren, und dass die meisten der kompromittierten Geräte in den USA liegen.

Im August 2016 berichteten Forscher, dass etwa eine Million mit dem Internet verbundene Videokameras und DVRs mit Malware infiziert waren. Die meisten Besitzer von Kameras und DVRs waren sich nicht bewusst, dass ihre Geräte infiziert sind.

Im Januar 2017 infizierten Internetkriminelle 70 Prozent der 187 Videospeichergeräte, die Daten von föderalen Überwachungskameras in Washington DC aufnahmen, vier Tage lang, kurz vor der Amtseinführung des Präsidenten, für eine Ransomware-Cyber-Attacke.

Diese und andere ähnliche Vorfälle sind der Beweis dafür, dass Video-Sicherheitssysteme für Hersteller von Sicherheits-Videogeräten, für die Installation von Sicherheitsintegratoren und für ihre Endkunden von größter Bedeutung sein sollten. Die Hackerverteidigung ist jedoch nur ein Teil, so dass Sicherheitsvideosysteme ihren

Zweck erfüllen können - die Aktivitäten innerhalb der Sichtfelder ihrer Kameras genau zu überwachen und aufzuzeichnen.

Video System Cyber- Sicherheit

Die Sicherheit von Computern und Netzwerken konzentriert sich auf den Schutz der Vertraulichkeit, Integrität und Verfügbarkeit (CIA) der vernetzten Systeme und der darin enthaltenen Daten. Diese drei Faktoren sind für Videosysteme von entscheidender Bedeutung, da das aufgezeichnete Videomaterial einer Kamera ein kritischer rechtlicher Beweis sein kann. Darüber hinaus sind die heutigen Videosysteme für viele Arten von Unternehmen betriebsrelevant geworden, sowohl für die sofortige Überwachungsfunktion, die sie bieten, als auch für die Geschäftseinblicke, die durch eine große Vielfalt von Videoanalysen ermöglicht werden. Überall und jederzeit ist die Verfügbarkeit von Videos über mobile Geräte eine grundlegende Geschäftserwartung.

Bei den meisten Videosystemen stellt jedoch die Internetkonnektivität ein Risiko für Vertraulichkeit, Integrität und Verfügbarkeit dar, da die meisten Systeme keinen integrierten Schutz vor Cyber-Angriffen bieten. Daher sind viele Videosysteme gegen Cyber-Angriffe wehrlos, obwohl die fortgesetzte Eskalation solcher Angriffe es für Videosysteme immer wichtiger macht, Cyber-sicher zu sein.

Mehrzweckprodukte und Spezialprodukte

Herkömmlicherweise wurden vernetzte Videomanagementsysteme aus Allzweckcomputern, Netzwerk-Switches, Routern und Firewalls aufgebaut, die eine erhebliche Menge an hochtechnischer Konfiguration benötigen, um als ein cybersicheres System zu arbeiten. Führende Hersteller bieten Anleitungen zur System- oder Gerätehärtung zum Einrichten geeigneter Cyber-Sicherheitssteuerelemente. Selbst dann ist die Sicherheit ein fortlaufendes Projekt, das ständige Aufmerksamkeit und Aktualisierung erfordert, da Produkte verbessert werden und neue Cyberbedrohungen entstehen.

Security firms report growing attacks from infected security cameras and DVRs, plus ransomware attacks on recorders

2015
- Number of botnet DDoS attacks highest in two years
- Attack sizes over 10 Gigabits per Second (Gbps)
- Majority of infected devices are cameras and DVRs

2016
AUG – Level 3 reports about 1 million compromisable brand name security cameras and DVRs
– Mirai botnet software appears, with variant named DvrHelper
SEP – 620 Gbps Mirai attack on KrebsOnSecurity site
– 1,100 Gbps Mirao attack on OVH web servers by more than 145 thousand cameras and DVRs
OCT – Mirai source code released online
– Level 3 reports Mirai botnet doubles in size from 213,000 to 493,000 devices
– 90% of infected devices are cameras and DVRs
– Dyn (internet DNS infrastructure provider) receives attacks from tens of millions of IP addresses, bogging down or taking offline major websites including AirBnB, Amazon, Etsy, Pinterest, Reddit, Netflix, PlayStation Network, SoundCloud, Spotify, and Twitter
NOV – Updated version of Mirai appears
– Almost 1 million Deutsche Telekom customers lose Internet service for two days

2017
JAN – Ransomware cyber attack infects 70% of DRVs of Washington D.C. public area police cameras, recording is offline for four days, just before Presidential Inauguration
MAY – Researcher discovers new malware (Persirai) that specifically targets 1,250 models of security cameras, from an unknown single overseas manufacturer, with over 185,000 already sold under various labels
JUL – Researchers discover a serious flaw (Devil's Ivy) in nearly all cameras supporting the ONVIF specification. It allows hackers to take full control of ONVIF-compliant cameras. Millions of installed cameras, including the top brands, are vulnerable.

Die Konfiguration eines sicheren VMS aus Allzweckgeräten ist für Installateure und Kunden von Videosystemen eine große Herausforderung, vor allem, weil dies nicht notwendig ist. Hersteller von speziell entwickelten Videoüberwachungsprodukten können und sollten vorkonfigurierte Systeme bereitstellen, da sie das Gerät entworfen und gebaut und die Software geschrieben haben, die gesichert werden muss. Darüber hinaus kann und sollte ein Cloud-basiertes Videoüberwachungssystem, das als Service bereitgestellt wird, die ständige Aufmerksamkeit und Aktualisierung enthalten, die ein effektiver Cyber-Sicherheitsschutz erfordert.

Im weiteren Verlauf dieses Artikels wird erläutert, wie Eagle Eye Networks den Cyber-Sicherheitsschutz anspricht und die Bereitstellung von Videosystemen mit einem speziellen Design vereinfacht.

Video System Cyber- Sicherheitslücken

Bei den meisten Cyber-Angriffen wird der Zugriff über Benutzeranmeldeinformationen ermöglicht. Anschließend werden Geräte- und Systemlücken ausgenutzt, um einen Zugriff zu erhalten, der den Angreifern die volle Kontrolle ermöglicht. Werkseitig voreingestellte Passwörter, einfach zu erratende Passwörter und Schwachstellen, die die Eskalation von Zugriffsrechten ermöglichen, sind die erfolgreichsten automatisierten und manuellen Cyber-Angriffe. Eine Suche nach "cameras DVRs DDoS" (ohne Anführungszeichen) auf der Website krebsonsecurity.com listet viele detaillierte Artikel über Sicherheits-Kameras und -Rekorder von gefährdeten Marken auf. Dies sind die Marken und Modelle von Kameras, die kompromittiert wurden und den Botnets beitreten mussten, die die DDoS-Attacken, die zuvor beschrieben wurden, erzeugten.

Botnet-Angriffe in großem Maßstab manifestieren sich aufgrund ihrer Größe und Auswirkung schnell und erregen erhebliche Aufmerksamkeit in den Medien. Unbemerkte manuelle Angriffe auf Videosysteme im kleinen Maßstab können jedoch für ein Unternehmen gefährlicher sein, beispielsweise indem sie einem Möchtegerndieb erlauben, ein Geschäft per Fernzugriff zu "vertuschen", indem sie Aktivitäten im Geschäft wie den Umgang mit Bargeld und die Warenlagerung betrachten.

Unautorisierte Zugriffe verhindern

Dank des selbstkonfigurierenden Systemdesigns von Eagle Eye Networks müssen sich Installateure nicht mehr bei Eagle Eye-Videogeräten anmelden, sodass die Anwendungen nicht die typischen Schwachstellen von Benutzername und Passwort aufweisen. Die Anwendungen verbinden sich automatisch mit dem Video Management System (VMS) der Eagle Eye Cloud-Überwachungskamera und ignorieren alle eingehenden Verbindungsanforderungen aus dem Internet.

Eagle Eye-Geräte isolieren die Kameras vom Internet. Da es keine Möglichkeit gibt, direkt aus dem Internet auf Kameras zuzugreifen, können Sicherheitslücken im Kamera-Passwort nicht durch internetbasierte Botnet-Malware oder manuelle Hack-Versuche aus der Ferne ausgenutzt werden.

Die Eagle Eye Anwendungen verwenden digitale Zertifikate, um verschlüsselte Datenverbindungen herzustellen und sich am Cloud Security Camera VMS im Eagle Eye Cloud Data Center zu authentifizieren. Auf Live- und aufgezeichnete Videos wird sicher über das Cloud Security Camera VMS zugegriffen, das die Wahl zwischen einer Zwei-Faktor- oder biometrischen Benutzerauthentifizierung bietet, um Benutzern Zugriff auf Kameras und aufgezeichnete Videos zu gewähren.

Eagle Eye Cyber Security Vorteile

Eagle Eyes gut konzipiertes Cloud-basiertes Video-Management-System bietet mehrere wichtige Vorteile für die Cyber-Sicherheit, die bei vollständig projektorientierten Systemen fehlen:

- **Starke Sicherheitsprofile.** Die starken physischen und Cyber-Sicherheitsprofile der hochsicheren Cloud-Datenzentren von Eagle Eye sind zu schwierig und kostenintensiv für die Implementierung für Videoüberwachungssysteme vor Ort, insbesondere für kleine Büros, Geschäfte, Servicezentren und

Produktionsstätten. Mit einem Cloud-basierten System teilen sich alle Kunden kostengünstig die hohe Sicherheit, die für den Live- und Videoaufzeichnungs-Zugriff bereitgestellt wird.

- **Verwaltete Systeme.** Die lokalen Video-Anwendungen von Eagle Eye werden vom Eagle Eye Cloud Data Center aus verwaltet und werden automatisch mit Sicherheits- und Feature-Updates auf dem neuesten Stand gehalten. Installateure und Kunden sind von dieser Belastung befreit.
- **System- und Datenspeicherung.** Die Server und Datenbanken von Eagle Eye befinden sich in mehreren Cloud-Rechenzentren, so dass die kontinuierliche Systembetriebszeit unabhängig vom Status eines einzelnen Servers oder Datenspeichers aufrechterhalten wird. Der lokale Videospeicher kann zusätzliche Speicherkapazität bieten.

Dank des Mobile Computing kann das Eagle Eye Cloud Camera Security VMS seine Verfügbarkeit jederzeit an jedem Ort, an dem auf das Internet zugegriffen werden kann, sicher erweitern. Die cloudbasierte Videoverwaltungssystem-Software Eagle Eye in Kombination mit Eagle Eye's eigenen Vor-Ort-Geräten, die als Abo-Modell bereitgestellt werden, stellt die kostengünstigste Möglichkeit dar, höchste Vertraulichkeit, Integrität und Verfügbarkeit für Überwachungsvideos zu erreichen .

Systemarchitektur

Die Eagle Eye Cloud-Überwachungskamera VMS ist ein cloud-gesichertes System, das herkömmliche DVRs (digitale Videorekorder) und NVRs (Netzwerkvideorekorder) ersetzt durch:

- **Vor-Ort-Eagle Eye Geräte.** Bridges zum Empfangen und Puffern von Video-, Audio-, Alarm- und Ereignisdaten von Kameras und Videoencodern und zum Senden an das Eagle Eye-Cloud-Datencenter und Cloud-verwaltete Videorekorder (CMVRs), die alle Bridge-Funktionen und den lokalen Speicher für Video vor Ort ausführen. Die erforderliche Netzwerk-, Routing- und Firewall-Funktionalität ist in die Anwendungenintegriert, um die Integrität der Vor-Ort-Komponenten sicherzustellen.
- **Eagle Eye's Rechenzentrumsausrüstung außer Haus.** Eagle Eye's Cloud-Überwachungskamera VMS Plattform und Video API Platform Anwendungsserver, Systemdatenspeicher und Videodatenspeicher, alle im Eagle Eye Cloud Data Center.

Das Eagle Eye-

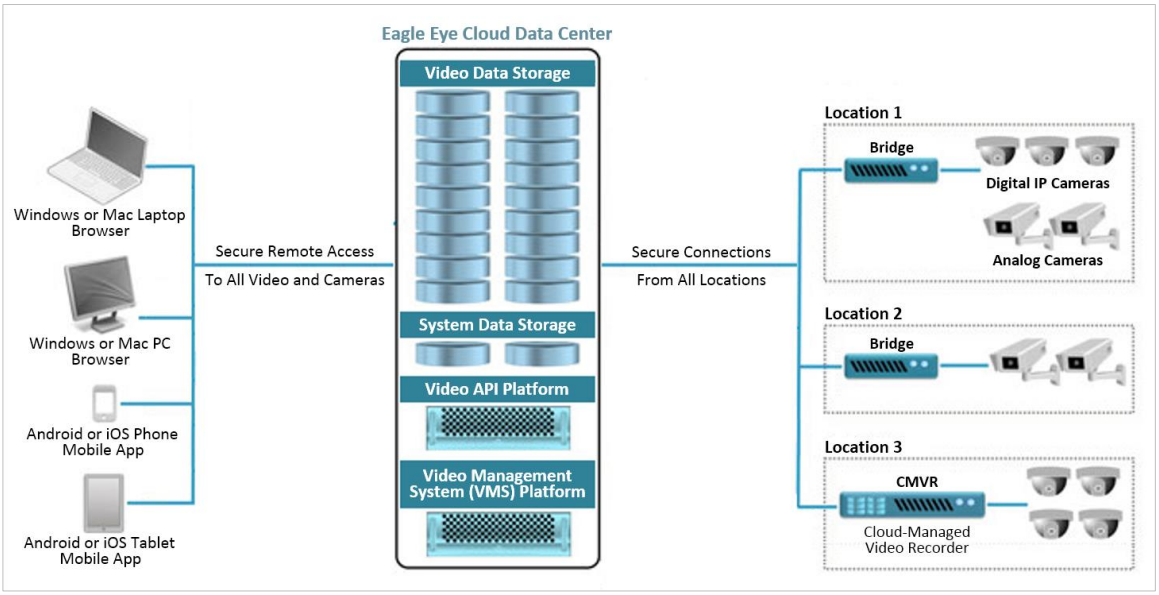


Figure 2. Eagle Eye Video Management System Architecture

System basiert vollständig auf einer modernen redundanten Cloud-Architektur, die eine webbrowserbasierte Oberfläche und umfassende mobile Anwendungen für iOS- und Android-Smartphones und -Tablet-Geräte bietet. Abbildung 2 zeigt die Systemarchitektur.

Die Aufzeichnung erfolgt in der Regel außerhalb des Eagle Eye Cloud Data Centers, kann jedoch auf Wunsch des Benutzers auch vor Ort durchgeführt werden, wo sich die Kameras befinden, oder eine Kombination der beiden Speicherorte pro Kamera verwenden. Wenn die Aufzeichnung außerhalb des Standortes erfolgt, puffert das lokale Eagle Eye-Gerät die Daten lokal, so dass keine Videos verloren gehen, wenn die Internetverbindung getrennt wird.

Kamera- und Datenisolierung

Sowohl bei der Aufzeichnung vor Ort als auch auß Haus sind die Kameras niemals direkt mit dem Internet verbunden. Für die externe Aufzeichnung aggregieren und puffern Eagle Eye Bridge-Anwendungen die Videodaten für die sichere verschlüsselte Übertragung an das Eagle Eye Networks Cloud Data Center. Für die lokale Aufzeichnung zeichnen Eagle Eye CMVRs lokal auf und stellen weiterhin sicher, dass die Kameras keine direkte Verbindung zum Internet haben. Dies gewährleistet ein hohes Maß an Sicherheit.

Eagle Eye Cloud Data Center

Im Zentrum der Systemarchitektur stehen hochsichere Rechenzentren, die miteinander kooperieren und sichere Verbindungen zu kundenseitigen Anwendungen aufrechterhalten. Die Datenzentren implementieren ein redundantes Datenspeicherschema, bei dem die Videodaten der Kunden auf drei verschiedenen Archivern gespeichert werden, so dass der Verlust eines aufgezeichneten Videos höchst unwahrscheinlich ist. Der Einfachheit halber werden diese Rechenzentren gemeinsam als Eagle Eye Cloud Data Center bezeichnet.

Das Rechenzentrumsdesign umfasst unterteilte Sicherheitszonen mit biometrischen Zugangskontrollen. Alle Komponenten des Rechenzentrums sind vollständig fehlertolerant, einschließlich redundanter Netzwerk-Uplinks, Anwendungsserver, Datenspeicher, Kühler, HVAC-Systemen, Power Panels und Stromverteilung. Die Netzwerkverteilung ist redundant, einschließlich Dual-Netzwerkkarten in Servern. Elektrische Energie wird von zwei verschiedenen Quellen zur Verfügung gestellt, z. B. zwei verschiedenen Versorgungsunterstationen, und zwei

Ersatzgeneratoren werden verwendet (einer für jede Stromquelle). Es gibt keinen einzigen Fehlerpunkt. Diese Anforderungen führen zu einer Verfügbarkeit der Hardware von 99,999%.

Die Eagle Eye Cloud Data Center-Standorte sind mit biometrischen Scannern und einem sicheren Kartenzugriff auf die Kollokationsdienste des Rechenzentrums ausgestattet. Sicherheitspersonal vor Ort überwacht die Hosting-Einrichtungen rund um die Uhr über Videoüberwachung im Innen- und Außenbereich. Der Zugang zum Rechenzentrum erfordert einen Check-in am Sicherheitsschalter und wird rund um die Uhr verwaltet. Die lokale Schlüsselverwaltung wird für Regale und Schränke durchgesetzt.

Der mehrschichtige Ansatz des Eagle Eye Cloud Data Centers zur Netzwerksicherheit umfasst Perimeterfirewalls, Einbruchspräventions-Systeme für das Netzwerk, Network Address Translation (NAT) und Netzwerksegmentierung, wobei Datenbankserver für die Öffentlichkeit nicht sichtbar sind. Außerdem sind Rechenzentrumsumgebungen sowohl logistisch als auch physisch vom Unternehmensnetzwerk von Eagle Eye getrennt. Der Internetzugang erfolgt über redundante Internet-Backbone- Netzwerke.
Eagle Eye verwendet für Eagle Eye-Mitarbeiter, die über einen physischen Zugang zu einem Rechenzentrum oder einen privilegierten logischen Zugriff auf die Eagle Eye Cloud Data Center-Plattform verfügen, umfangreiche Screenings und Hintergrundprüfungen.

Eagle Eye Vor-Ort- Anwendungen

Eagle Eye-Anwendungen puffern Videos lokal und senden sie mithilfe der Intelligent Bandwidth Management ™ - Technologie von Eagle Eye an die Eagle Eye-Cloud, die speziell auf die begrenzte Bandbreite abgestimmt ist. I

Das Intelligent Bandwidth Management passt die Datenübertragung und die Bandbreitennutzung dynamisch an und priorisiert Übertragungen, um die bestehende Internetverbindung optimal zu nutzen. Wie bereits in Abbildung 2 gezeigt, gibt es zwei Kategorien von Eagle Eye-Geräten:

- *Bridges*, die Videos puffern und an die Cloud senden, die Verschlüsselung, Videodeduplizierung, Bandbreitenverwaltung, Bewegungsanalyse und Videokomprimierung durchführen; und
- *Cloud-verwaltete Videorekorder* (CMVRs), die alle Funktionen einer Bridge ausführen und Videomaterial lokal aufzeichnen und optional in die Cloud senden.

Sowohl Standalone- als auch Eingebaute-Versionen der Eagle Eye-Anwendungen erfordern keinen Netzwerkswitch oder Router eines Drittanbieters, um die Kameras in ihrem eigenen Netzwerk zu isolieren und ihre Videodaten zu verschlüsseln und an das Eagle Eye Cloud Data Center zu senden. Jede Anwendung verfügt über mindestens zwei Netzwerkanschlüsse, einen für das Kameranetzwerk und einen für die Verbindung mit dem Internet. Die Anwendungen enthalten die erforderliche Netzwerk-, Routing- und Firewall-Funktionalität. Einige Anwendungen verfügen über zusätzliche POE-Netzwerkports für den Anschluss an einzelne Kameras, um den Fernauslöser für jede Kamera zu ermöglichen.

Einfache und sichere Bereitstellung

Die sichere Bereitstellung von Eagle Eye-Anwendungen ist einfach, da sie alle als "gesperrte" Geräte konzipiert sind, keine offenen Ports haben, keine eingehende Kommunikation akzeptieren und für die automatische Authentifizierung und Verbindung mit dem Eagle Eye Cloud Security Camera VMS vorkonfiguriert sind. Zum

Herstellen von Netzwerkverbindungen ist keine Konfiguration erforderlich. Kameras werden automatisch erkannt und müssen manuell genehmigt werden, bevor sie im System registriert werden. Bridges und CMVRs fungieren als DHCP-Server für Netzwerkkameras, so dass keine Kamera-IP-Adressen manuell festgelegt werden müssen.

Cyber-Sicherheitsfeatures

Die Cloud-basierte, speziell entwickelte VMS-Infrastruktur von Eagle Eye bietet hohe Sicherheit für Vertraulichkeit, Integrität und Verfügbarkeit von Überwachungsvideos unter Verwendung verschiedener standardbasierter Best Practices für die Cyber Sicherheit. In den folgenden Abschnitten wird beschrieben, wie die Verschlüsselung und digitale Zertifikate von der Cloud-Überwachungskamera-VMS-Infrastruktur von Eagle Eye verwendet werden. Zusätzliche Sicherheitsmaßnahmen der Eagle Eye-Organisation und ihrer Technologieinfrastruktur werden ebenfalls beschrieben.

Eagle Eye Datenverschlüsselung

Bei der Verschlüsselung werden Daten so abgeändert, dass sie unlesbar sind (Verschlüsselung), so dass sie in ihre lesbare Form zurückgeführt werden können (Entschlüsselung). Die einfachste Art der Verschlüsselung verwendet einen einzelnen Satz von Zeichen (Zahlen, Buchstaben und / oder Symbole) - den Sschlüssel - zum Verschlüsseln und Entschlüsseln der Daten.

Eagle Eye verwendet eine Technik namens Public Key Encryption, die auf einer mathematischen Tatsache basiert, dass ein Paar sehr großer Zahlen eine spezielle Beziehung zueinander haben kann, wobei das, was Sie mit einer Zahl verschlüsseln (mit speziellen Methoden) nur mit der anderen Zahl verschlüsselt und entschlüsselt werden kann. Wenn Sie jedoch ein andere Nummer nutzen, können Sie die andere Nummer nicht herausfinden. Diese einfache, aber unzerbrechliche Beziehung zwischen den Nummern ermöglicht viele Arten von Vertrauensbeziehungen und Datenschutzfähigkeiten.

Die Verschlüsselung mit einem öffentlichem Schlüssel ist der Kurzname für die Verschlüsselung mit einem öffentlichem / privatem Schlüssel. Wenn ein Schlüssel privat gehalten wird und nur der andere Schlüssel (der öffentliche Schlüssel) freigegeben wird, werden zwei wichtige Funktionen eingerichtet:

- **Quellenauthentizität.** Informationen, die mit einem privaten Schlüssel verschlüsselt werden, können mit dem entsprechenden öffentlichen Schlüssel gemeinsam genutzt und entschlüsselt werden, wodurch die Quelle - der Inhaber des privaten Schlüssels - überprüft wird.
- **Datenschutz.** Das Verschlüsseln von Informationen mit einem öffentlichen Schlüssel stellt sicher, dass nur eine Person (oder ein System) sie entschlüsseln kann - der Inhaber des privaten Schlüssels.

Wann immer wir den Begriff "öffentlicher Schlüssel" sehen, wissen wir, dass auch ein privater Schlüssel involviert ist.

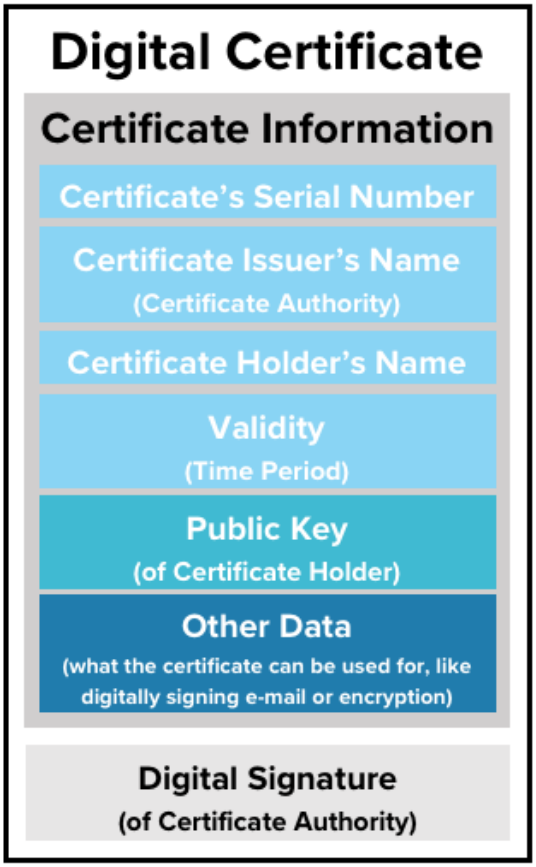
Öffentliche und private Schlüssel verwalten

Woher kommen öffentliche / private Schlüsselpaare? Wie werden Schlüssel sicher verteilt? Diese und andere Probleme werden durch den ANSI X.509-Standard für eine Public-Key-Infrastruktur (PKI) für digitale Zertifikate, die Public-Key-Verschlüsselung und das Public-Key-Management behoben.

Digitale Zertifikate

Digitale Zertifikate sind kleine elektronische Dokumentdateien. Jede Datei enthält Informationen, die zum Nachweis der Authentizität und Integrität der digitalen Zertifikatsdatei und ihrer Daten verwendet werden können. Öffentliche Schlüssel sind Teil der Informationen in einem digitalen Zertifikat, wie in Abbildung 3 gezeigt.

Figure 3. Example of Digital Certificate



Verwendung für digitale Zertifikate

Ein digitales Zertifikat listet die Verwendungen auf, die der Zertifikatsinhaber dafür vorsieht, wie z.B.

- Stellt die Identität eines Fern-Computers sicher
- Beweist Ihre Identität einem Fern- Computer
- Stellt sicher, dass die Software vom Software-Herausgeber stammt
- Schützt die Software vor Änderungen nach der Veröffentlichung
- Schützt E-Mail-Nachrichten
- Ermöglicht das Signieren von Daten mit der aktuellen Uhrzeit
- Ermöglicht das Verschlüsseln von Daten auf der Festplatte
- Ermöglicht eine sichere Kommunikation im Internet

Eagle Eye verwendet digitale Zertifikate, um gespeicherte Daten zu verschlüsseln und sichere Verbindungen zwischen Benutzern und dem Eagle Eye Cloud Security Camera VMS sowie zwischen Eagle Eye-Anwendungen und dem VMS herzustellen.

Eagle Eye's Verwendung von digitalen Zertifikaten

Eagle Eye verwendet digitale Zertifikate, die durch den ANSI X.509-Standard beschrieben werden, der eine Certificate Authority (CA) - eine vertrauenswürdige Partei, die die Identität von Zertifikatsinhabern vor ihrer Ausstellung extern validieren kann - zur Erstellung, Verwaltung und Sperrung von Zertifikaten benötigt.

Für die Authentifizierung von Verbindungen mit dem Eagle Eye Cloud-Überwachungskamera-VMS verwendet Eagle Eye digitale Zertifikate, die von einer anerkannten Zertifizierungsstelle von Drittanbietern ausgestellt wurden, deren Zertifikate den wichtigsten Webbrowsern vertrauen.
Für die Authentifizierung von Verbindungen zu Eagle Eye-Anwendungen agiert Eagle Eye als eigene Zertifizierungsstelle und stellt eigene Zertifikate aus, denen Eagle Eye vertrauen kann, da es eine physische Überwachungskette bei der Installation von Zertifikaten in die Anwendungen als Teil des Herstellungsprozesses

gewährleisten kann . Dies funktioniert, da nur Eagle Eye-Systeme und -Geräte Teil der Authentifizierungsprozesse sein können, die die digitalen Eagle Eye-Zertifikate verwenden.

Eagle Eye Cloud Data Center-Authentifizierung

Für die Kommunikation mit dem Browser und der mobilen App verwendet der Eagle Eye Cloud Data Center-Server, wie bereits erwähnt, ein digitales Zertifikat eines Drittanbieters, um die sichere TLS-Verbindung herzustellen. Die meisten Browser ermöglichen das Anzeigen des Inhalts des Zertifikats, das zum Herstellen der Verbindung verwendet wird, so dass Nutzer überprüfen können, ob sie tatsächlich mit einem tatsächlichen Eagle Eye Cloud Data Center-Server verbunden sind.

Eagle Eye Anwendungs-Authentifizierung

Wie bereits erwähnt, verwenden Eagle Eye-Anwendungen selbstsignierte digitale Zertifikate, um sich beim Eagle Eye Cloud Data Center zu authentifizieren.

Übertragene Datenverschlüsselung

Die Eagle Eye-Webanwendung, mobile Apps und APIs kommunizieren über HTTPS mithilfe von TLS (Transport Layer Security). Das TLS-Protokoll zielt hauptsächlich darauf ab, Datenschutz und Datenintegrität zwischen zwei kommunizierenden Computeranwendungen bereitzustellen. TLS erreicht dies auf drei Arten:

- Authentifizieren der kommunizierenden Anwendungen mit digitalen Zertifikaten.
- Sicherstellung, dass die Verbindung privat ist, indem sie eine starke Datenverschlüsselung verwenden.
- Einschließen einer Nachrichtenintegritätsprüfung unter Verwendung eines Nachrichtenauthentifizierungscodes, um einen unbemerkten Verlust oder eine Veränderung der Daten während der Übertragung zu verhindern.

Die Eagle Eye-Webanwendung, mobile Apps und APIs verwenden die TLS Version 1.1 oder höher unter Verwendung des sicheren SHA-256-Hashalgorithmus mit einem 2048-Bit-RSA-Schlüssel.

Gespeicherte Datenverschlüsselung

Gespeicherte Daten werden mit der AES-256-Bit-Verschlüsselung (Advanced Encryption Standard) sowohl auf den Bridges als auch im Eagle Eye Cloud Data Center geschützt. Schlüssel werden mit digitalen Eagle Eye-Zertifikaten gespeichert und ausgetauscht.

Benutzerauthentifizierung

Das Eagle Eye Camera Security VMS bietet verschiedene Arten des sicheren Anmeldezugriffs für Benutzer:

- Benutzer Zwei-Faktor-Authentifizierung
- Apple Touch ID Fingerabdruck-Authentifizierung
- Echtzeit-Videozugriff für designierte Personen

Benutzer Zwei-Faktor-Authentifizierung

Benutzer sind Mitarbeiter von Eagle Eye-Kunden mit zugewiesenen Rechten zur Anmeldung bei Eagle Eye-Anwendungen (mobile Apps oder Browser-Apps), um auf Videos zuzugreifen oder Kameras zu verwalten. Die Zwei-Faktor-Authentifizierung wird verwendet, um eine starke Sicherheit zu bieten, indem vertrauenswürdige Benutzergeräte (PCs, Laptops, Tablets und Smartphones) eingerichtet werden und nur der Kamera- und Videozugriff von diesen vertrauenswürdigen Geräten aus ermöglicht wird. Versuche, sich mit einem nicht vertrauenswürdigen Gerät anzumelden, führen dazu, dass der Zugriff verweigert wird.
Die Zwei-Faktor-Authentifizierung nutzt die folgenden Mechanismen:

- **Vertrauenswürdiges Gerät.** Ein vertrauenswürdiges Gerät ist ein mobiles Gerät oder ein Browser auf einem bestimmten Computer, der zuvor mithilfe der Zwei-Faktor-Authentifizierung registriert wurde. Es ist ein Gerät, von dem bekannt ist, dass es mit diesem Eagle Eye-Benutzer verknüpft ist.
- **Sicherheitscode.** Ein Sicherheitscode ist ein einmalig verwendeter Code, der an ein vertrauenswürdiges Gerät oder eine vertrauenswürdige Telefonnummer gesendet wird, wenn sich der Benutzer zum ersten Mal mit einem neuen Gerät oder Browser anmeldet.

Apple Touch ID Fingerabdruck-Authentifizierung

Das Eagle Eye VMS unterstützt die Fingerabdruck-Biometrie von Apple Touch ID, um die Wahrscheinlichkeit zu minimieren, dass Dritte die Passworteingabe beobachten, und um die Anmeldung sicherer und bequemer zu machen. Der Mechanismus nutzt den iOS Keychain-Passwortspeicher und ermöglicht die Verwendung des Fingerabdrucks des Benutzers für die Anmeldung.

Echtzeit-Videozugriff für designierte Personen

Das Eagle Eye Cloud-Überwachungskamera-VMS ermöglicht es Kunden, designierte Personen im Voraus zu bestimmen, die in Notfallsituationen über die kostenlose mobile Eagle Eye Viewer-App oder einen beliebigen gängigen Webbrowser sofortigen Zugriff auf Echtzeitkameras erhalten. Kunden geben außerdem an, welche ihrer eigenen Mitarbeiter berechtigt sind, den Notfalldienst zu aktivieren, wenn ein Vorfall eintritt.

Die Erlaubnis des Notfallhelfers kann auf bestimmte Gruppen von Kameras beschränkt sein; beispielsweise nur für Außenkameras und öffentliche Lobbybereiche. Die Kameras werden privat gehalten und nur freigegeben, wenn ein autorisierter Benutzer den Zugriff des Notfallhelfers aktiviert. Wenn der Notfallhelfer-Zugriff aktiviert ist, erhalten die Notfallhelfer eine E-Mail mit Links zu bestimmten Kameras, die sie anzeigen dürfen. Die Links öffnen die Kameraansichten in der App oder im Webbrowser.

Anwendungssicherheit

Das Betriebssystem, der Webserver und die Anwendungssoftware werden auf dem neuesten und sichersten Stand gehalten

Software. API-Sicherheit wird sowohl für Eagle Eye-Anwendungen als auch für API-Integrationen von Drittanbietern implementiert. Eagle Eye führt als Teil des Entwicklungsprozesses Penetrationstests und Anwendungsscans durch. Darüber hinaus werden regelmäßige Penetrationstests mit dem Eagle Eye Cloud Security Camera VMS durchgeführt. In regelmäßigen Abständen werden potenzielle Kunden, die über interne Penetrationstests verfügen, die Erlaubnis erhalten, eine Penetration mit der Eagle Eye Cloud Security Camera VMS durchzuführen.

Schutz von Kundendaten

Hardware- und Softwarekonfigurationen sowie mandantenunabhängige Sicherheitskontrollen halten Kundendaten getrennt. Jeder Kunde kann nur sein eigenes Live- und aufgezeichnetes Videomaterial und Systeminformationen

anzeigen. Bei der Verbindung mit dem Eagle Eye Cloud-Überwachungskamera-VMS hat kein Kunde Einblick in das System eines anderen Kunden und kann nicht auf andere Kundendaten zugreifen.

Erweiterte Netzwerkanforderungen

Einige Einrichtungen, insbesondere kritische Infrastruktureinrichtungen, werden von hochgradig fähigen IT-Abteilungen unterhalten, die ihre eigene Netzwerkinfrastruktur für Videokameras für Sicherheitskameras bevorzugen. In solchen Fällen arbeitet Eagle Eye in Bezug auf Netzwerkanforderungen mit ihnen zusammen, um sicherzustellen, dass die Standards und Verfahren für Kundennetzwerke bei der Bereitstellung des Eagle Eye Cloud Security Camera VMS angemessen angewendet werden.

Eagle Eye Sicherheitspraktiken

Eagle Eye wendet beim Umgang mit Kundeninformationen strenge Datenschutz- und Informationssicherheitsstandards an. Unsere Kundenverträge beinhalten Vertraulichkeitsbestimmungen, die uns die Offenlegung vertraulicher Informationen unserer Kunden untersagen, außer unter bestimmten Umständen, wie gesetzlich vorgeschrieben. Unsere Mitarbeiter unterzeichnen Vertraulichkeitsvereinbarungen, werden geschult und befolgen unsere Datenschutz- und Sicherheitsrichtlinien und -verfahren. Zum Beispiel erfordert die Passwortverwaltungsrichtlinie, dass starke, nicht leicht zu erratende Passwörter verwendet werden, dass Passwörter häufig geändert werden und dass Passwörter nirgendwo niedergeschrieben werden.

Eagle Eye hat Richtlinien veröffentlicht, und fordert alle Benutzer von jeder Art von Sicherheits-Kamera-System auf, die Richtlinien für die Sicherheit von Cyber-Kameras zu befolgen.

Zusammenfassung der technischen Cyber-Sicherheitsmaßnahmen

Die folgenden Listen fassen die technischen Maßnahmen zur Cybersicherheit zusammen, die in diesem Dokument beschrieben werden:

Vor-Ort-Ausrüstung für die Cyber-Sicherheit

- Keine eingehenden Internetverbindungen werden akzeptiert
- Kameras sind vom Internet isoliert
- Anwendungen haben keine offenen Netzwerkports
- Anwendungen sind gegen vorinstallierte Kamera-Malware geschützt

- Anwendungen verwenden TLS-Verbindungen zur Eagle Eye Cloud Security Camera VMS
- Verschlüsselung wird auf gepuffertes und lokal aufgezeichnetes Video angewendet
- Anwendungs-Authentifizierung über digitale Zertifikate
- Zusammenarbeit in Bezug auf erweiterte Netzwerkanforderungen von Kunden

Physische Sicherheit des Datenzentrums

- Alarmsystem für die Einbruchmeldung

- Zugangskontrolle für biometrische Einrichtungen
- 24/7 Sicherheitspersonal vor Ort
- 24 Stunden Vor-Ort-Live- und Videoaufzeichnung
- Sicherheitsdesk Besucheridentitätsüberprüfung und Besucherprotokoll
- Biometrische physische Zugangskontrolle
- Die lokale Schlüsselverwaltung wird für Regale und Schränke durchgesetzt
- Umfangreiche Screening- und Hintergrundprüfungen für Eagle Eye-Mitarbeiter mit Data Center- oder Eagle Eye Cloud Security Camera VMS-Zugriff.
- Data- Center-Netzwerksicherheit
- Netzwerkperimeter-Firewalls
- Netzwerk-Einbruchspräventions-Systeme
- Netzwerkadressübersetzung (NAT)
- Netzwerksegmentierung, um Datenbankserver zu isolieren
- Logische und physische Trennung von Rechenzentrumsumgebungen vom Eagle Eye-Unternehmensnetzwerk

Redundanz

- Eagle Eye Cloud Security Camera VMS-Komponenten sind redundant (aktiv / aktiv oder aktiv / passiv)
- Dreifach redundanter Videodatenspeicher

Anwendungs- und Datensicherheit

- Regelmäßiger Server-Sicherheitslücken-Scan
- Regelmäßige Penetrationstests
- Sicherheit auf API-Ebene
- Web- und mobile Anwendungen verwenden eine Zwei-Faktor-Authentifizierung
- Verwendung der Fingerabdruckauthentifizierung für mobile Geräte
- Web- und mobile Anwendung nutzen TLS-Verbindungen zu Eagle Eye Cloud Security Camera VMS
- AES-Verschlüsselung von aufgezeichnetem Video
- Mandantenfähige Datensicherheitskontrollen

Fazit

Eagle Eye Networks hat die Cybersicherheitsrisiken von Videoüberwachungssystemen erheblich reduziert durch:

Entwerfen und Erstellen von hochsicheren Rechenzentren basierend auf einer modernen redundanten Cloud-Architektur

Entwicklung eines Cyber-sicheren cloudbasierten Überwachungskamera-Videoverwaltungssystems mit standardbasierter Verschlüsselung von Videodaten und sicherer Authentifizierung von Benutzern und mobilen Geräten

Speziell entwickelte, selbstkonfigurierende, sichere Video-Anwendungen, die Kameras von Internet-Cyber-Bedrohungen isolieren

Verwalten der Sicherheit und der Feature-Updates der Eagle Eye-Anwendung erfolgt automatisch, ohne dass ein Installationsprogramm oder eine Endbenutzeraktion erforderlich ist.

Damit bietet Eagle Eye die kostengünstigste Möglichkeit, die höchste Vertraulichkeit, Integrität und Verfügbarkeit von Überwachungsvideos zu erreichen, da es sich um einen gut verwalteten Abonnementdienst handelt.

Über Eagle Eye Networks

Eagle Eye Networks, Inc. ('Eagle Eye') wurde 2012 gegründet und ist der weltweit führende Anbieter von Cloud-basierten Videoüberwachungslösungen für Unternehmen, Alarm-Unternehmen, Sicherheitsintegratoren und Einzelpersonen. Eagle Eyes 100% cloud-verwaltete Lösungen bieten Cloud- basierte und Vor- Ort-Aufzeichnungen, Sicherheit und Verschlüsselung auf Bankenebene sowie umfassende Unterstützung für analoge und digitale Kameras - alles über das Internet oder mobile Anwendungen. Unternehmen aller Größen und Typen nutzen Eagle Eye-Lösungen für ihre betriebliche Optimierung und Sicherheit. Alle Eagle Eye-Produkte profitieren von der entwicklerfreundlichen RESTful-API-Plattform von Eagle Eye und dem Big Data Video Framework ™, der das Indizieren, Suchen, Abrufen und Analysieren von Live- und archivierten Videos ermöglicht. Die offene Video-API von Eagle Eye wurde weitgehend für die Integration in die Alarmüberwachung, Analyse von Drittanbietern, Sicherheits-Dashboards und Integration von Kassensystemen im Verkauf eingesetzt.

Eagle Eye verkauft seine Produkte über autorisierte globale Wiederverkäufer und Installationspartner. Eagle Eye mit Hauptsitz in Austin, Texas, USA, verfügt über Niederlassungen in Europa und Asien.

Über Dean Drako

Eagle Eye Networks wurde von Dean gegründet und ist das erste cloudbasierte Videoüberwachungsunternehmen, das Cloud- und Vor-Ort-Aufzeichnungen anbietet.

Dean hat während seiner eindrucksvollen Karriere führende Sicherheitsfirmen geleitet und führt diese auch weiterhin. Parallel zu Eagle Eye Networks ist Dean der Eigentümer und Vorsitzende von Brivo, einer Cloud-Zugangskontrollfirma. Zuvor gründete Dean als Gründer, Präsident und CEO von Barracuda Networks die erste E-Mail Sicherheitsanwendung der Branche. Vor Barracuda Networks gründete Dean Boldfish, einen führenden Anbieter von Outbound-E-Mail-Lösungen für Unternehmen, der 2003 von Siebel Systems übernommen wurde. Dean war Gründer, President und CEO von Design Acceleration, Inc. (DAI), einem Hersteller von erstklassigen Design-Analysen und Verifikations-Tools, die 1998 von Cadence Design Systems übernommen wurden.

Dean erhielt seine BSEE von der University of Michigan, Ann Arbor und MSEE von der University of California, Berkeley.

Goldman Sachs ernannte Dean zu einem der "100 faszinierendsten Unternehmer des Jahres 2014".

US Büro

Eagle Eye Networks
4611 Bee Caves Rd.
Suite 200
Austin, TX 7874
Tel: +1-512-473-0500
Web: www.een.com
Sales: sales@een.com

EMEA Büro

Eagle Eye Networks B.V.
Hogehilweg 19
1101 CB
Amsterdam
The Netherlands
Tel: +31 (0) 20 26 10 460
Sales: EMEAsales@een.com