EAGLE EYE NETWORKS

SICHERE CLOUD-VIDEOÜBERWACHUNG

Eagle Eye Networks Cybersicherheitsleitfaden

INHALTSVERZEICHNIS

Die Sicherheit von Videoüberwachungssystemen sollte innerhalb der Branche umfassender behandelt werden. Dadurch wird vermieden, dass Cybersicherheit als Problem für Systemintegratoren, Installateure oder Kunden zurückbleibt.

Eagle Eye Networks ist in dieser Hinsicht führend und mildert Sicherheitsbedenken, beginnend mit der Systemgestaltung und bis hin zur kontinuierlichen Cybersicherheitsverwaltung in der Cloud. Das Eagle Eye Cloud VMS (Videoverwaltungssystem) ist so konzipiert, dass es vor Systemschwachstellen schützt und automatische System-Sicherheitsupdates über die Cloud durchführt.

Einführung

Cyberkriminelle können Unternehmen jeder Größe und zu jeder Zeit angreifen. Kriminelle nutzen jede potenzielle Schwachstelle, um in das Netzwerk eines Unternehmens einzudringen und auf Identitäts-, Gehalts-, Kreditkarten- und andere wichtige Daten zuzugreifen. Die Häufigkeit von Angriffen und Sicherheitsverletzungen nimmt jedes Jahr zu, ebenso wie die damit verbundenen Kosten. Laut dem jährlichen IBM-Bericht über die Kosten von Datenschutzverletzungen, in dem Sicherheitsverletzungen bei Unternehmen aller Größenordnungen analysiert wurden, liegen die durchschnittlichen Kosten einer Datenschutzverletzung weltweit bei über 4 Millionen US-Dollar.

Unternehmen jeder Größe sind auf ein Netzwerk miteinander verbundener Systeme angewiesen, und jedes dieser einzelnen Systeme kann Sicherheitslücken aufweisen. Ein sicheres vernetztes System eliminiert so viele Risiken wie möglich, um die Vertraulichkeit, Integrität und Verfügbarkeit (CIA) des Systems und der darin enthaltenen Daten zu schützen.

Mit dem Netzwerk verbundene Videoüberwachungssysteme sind nicht immun gegen Cyberbedrohungen. Seit Jahren werden Überwachungskameras und -aufzeichnungsgeräte von Hackern als Waffe eingesetzt, um DDoS-Angriffe (Distributed Denial of Service) auf bestimmte Systeme auszuführen, die sich auf Unternehmen jeder Größe auswirken.

Abbildung 1 zeigt einige der bemerkenswertesten Cyberangriffe und Schwachstellen, die in den letzten Jahren Internet-verbundene Sicherheitskameras und digitale Videorekorder (DVRs) betroffen haben. Diese und ähnliche Vorfälle machen deutlich, dass Videoüberwachungssysteme weiterhin bedroht sind.

2021	MAR	Ein massiver Einbruch bei der Sicherheitsfirma Verkada hat die Live-Übertragungen von 150.000 Überwachungskameras in Krankenhäusern, Unternehmen, Polizeidienststellen, Schulen und anderen Einrichtungen offengelegt und damit die Privatsphäre von Kunden, Patienten und anderen gefährdet.
	JUL	Schwerwiegende, angreifbare Firmware-Schwachstellen wurden in der IP-Kamera-Firmware von UDP Technology entdeckt, die in Dutzenden von Überwachungsprodukten von Anbietern verwendet wird, wodurch die Sicherheitsgrundlage der dem Internet ausgesetzten Kamera-Infrastruktur offengelegt wird.
2022	APR	Die BotenaGo-Malware-Variante zielt auf Lilin-DVRs ab, um sie mit dem Mirai-Botnet zu infizieren, ihre Funktionalität einzuschränken und diese DVRs in Quellen für Angriffe auf andere Netzwerke zu verwandeln.
	JUN	Der rekordbrechende DDoS missbrauchte HTTP/2-Multiplexing (von Geräten, darunter Sicherheitskameras eines ungenannten chinesischen Telekommunikationsunternehmens), um 25,3 Milliarden Anfragen zu senden, die Kameranetzwerke zu stören und die Netzwerkbandbreite zu beeinträchtigen.
	AUG	Trotz verfügbarer Sicherheitsupdates wurden viele der 80.000 ungepatchten Hikvision-Kameras in 20.000 Unternehmen als Teil eines Mirai-basierten Botnetzes verwendet.
2023	FEB	Schwachstelle ermöglicht Hackern, Dahua-Sicherheitskameras aus der Ferne zu manipulieren und so die Sicherheit und Verfügbarkeit der betroffenen Kameras zu gefährden

Abbildung 1. Zeitleiste: Anhaltende Cyberangriffe auf Sicherheitsvideokameras und DVRs.

CYBER-SCHWACHSTELLEN IN VIDEOSYSTEMEN

Moderne Videoüberwachungssysteme sind nützlich, da sie über leistungsstarke Prozessoren und umfangreiche Netzwerkfunktionen verfügen, sowohl kabelgebunden als auch drahtlos. Für viele Videosysteme stellt die Internetverbindung jedoch ein Risiko für die Vertraulichkeit, Integrität und Verfügbarkeit (CIA) dar, da viele Systeme nicht über einen eingebauten Schutz vor Cyberangriffen verfügen. Angesichts der zunehmenden Zahl von Angriffen ist es wichtiger denn je, dass Videosysteme cybersicher sind.

Fehlkonfigurationen, Angriffe von Cyberkriminellen und Fehler in der konventionell installierten Kamera-Infrastruktur können wertvolle Videoinformationen und andere Daten offenlegen.

Bei vielen Cyberangriffen verschaffen sich die Angreifer über Phishing-Versuche oder Benutzeranmeldedaten Zugang und nutzen dann Schwachstellen in Geräten und Systemen aus, um ein hohes Maß an Zugriff zu erlangen, das den Angreifern volle Kontrolle ermöglicht. Werkseitig voreingestellte Passwörter, leicht zu erratende Passwörter und im Klartext übermittelte Passwörter, die eine Ausweitung der Zugriffsrechte ermöglichen, sind die Ursache für die meisten automatisierten und manuellen Cyberangriffe.

DVRs (digitale Videorekorder) und NVRs (Netzwerk-Videorekorder) benötigen in der Regel manuelle System-Sicherheitsaktualisierungen, die oft einen geplanten Besuch eines Technikers vor Ort erfordern. Diese Sicherheitspatches werden oft übersehen oder in einigen Fällen vom Hersteller nicht bereitgestellt, was zu einer Schwachstelle im System führt.

IST IHRE KAMERAINFRASTRUKTUR SICHER?

Hier sind einige Ressourcen, die Sie verwenden können, um Ihr bestehendes Kamera-Sicherheitssystem auf potenzielle Mängel zu überprüfen:

- Suchen Sie nach Informationen zu Sicherheitslücken auf sicherheitsorientierten Websites wie z. B. **Krebsonsecurity.com** Verwenden Sie Suchbegriffe wie „Kamera-Schwachstelle" oder „NVR DDoS", um detaillierte Artikel zu Sicherheitslücken zu finden.
- **Allgemeine Internetsuche:** Suchen Sie nach dem Hersteller Ihrer Kamera, um allgemeine Informationen zu erhalten, oder suchen Sie den Produktnamen oder das Modell, um spezifische Sicherheitswarnungen zu erhalten.
- **Achten Sie auf der Website des Herstellers** auf Sicherheitswarnungen oder Firmware-Updates, oder melden Sie sich für direkte Benachrichtigungen an.
- Überwachen Sie die Website des Herstellers auf Sicherheitswarnungen oder Firmware-Updates, oder melden Sie sich für direkte Benachrichtigungen an. Besuchen Sie öffentliche Websites wie die der US-Regierung **Agentur für Cybersicherheit und Infrastruktursicherheit (CISA),** wo Sie nach allgemeinen Begriffen (z. B. „Videoüberwachung") suchen können, um genauere Informationen zu erhalten.

CYBERSICHERHEIT VON VIDEOSYSTEMEN

In der Regel bestehen Videoüberwachungssysteme aus Universalcomputern, Netzwerk-Switches, Routern und Firewalls, die eine hochtechnische Konfiguration und ständige, manuelle Software- und Firmware-Sicherheitsupdates erfordern, um als cybersicheres System zu funktionieren. Die Konfiguration eines sicheren Videoüberwachungssystems auf der Grundlage von Universalgeräten ist eine große Herausforderung für Installateure und Kunden von Videosystemen - vor allem, wenn es eine einfachere Lösung gibt.

Die Hersteller von speziell entwickelten Videoüberwachungsprodukten können und sollten sichere, vorkonfigurierte Systeme anbieten, anstatt die Cybersicherheit als Problem den Systemintegratoren, Installateuren oder Kunden zu überlassen. Schließlich haben sie die Geräte entwickelt und gebaut und die Software entwickelt, die abgesichert werden muss. Darüber hinaus kann und sollte ein Cloud-basiertes Videoüberwachungssystem, das als Dienst bereitgestellt wird, die stetige Überprüfung und Updates beinhalten, die für einen wirksamen Schutz der Cybersicherheit erforderlich sind.

Das Eagle Eye Networks Cloud VMS (Video Management System) ist eine speziell entwickelte Cloud-Videoüberwachungslösung, die das Risiko bekannter Schwachstellen in Überwachungssystemen reduziert. Das abonnementbasierte VSaaS-Modell bietet automatische Sicherheitsupdates, und ein Expertenteam ist für die kontinuierliche Cybersicherheit der Cloud verantwortlich, wodurch ein Höchstmaß an Vertraulichkeit, Integrität und Verfügbarkeit (CIA) für Überwachungsvideos erreicht wird.

Im Folgenden wird erläutert, wie Eagle Eye Networks den Schutz vor Cyberangriffen gewährleistet und die Bereitstellung von Videosystemen durch ein speziell entwickeltes Design vereinfacht.

Eagle Eye Cybersicherheitsleistungen

Eagle Eye Networks verpflichtet sich zur Cybersicherheit und hat die SOC 2 Typ 2 Konformität abgeschlossen, die als höchster Standard für unabhängige Sicherheitsprüfungen gilt. Das Unternehmen hat auch die Konformität mit den umfassenden Sicherheitsstandards der ISO 27001:2013 abgeschlossen. Eagle Eye wendet beim Umgang mit Kundendaten strenge Datenschutz- und Informationssicherheitsstandards an. Unsere Mitarbeiter werden gründlich überprüft und unterzeichnen Vertraulichkeitsvereinbarungen, und werden in unseren Datenschutz- und Sicherheitsrichtlinien geschult und befolgen diese.

SYSTEMÜBERSICHT UND ARCHITEKTUR

Das Eagle Eye Cloud VMS ist eine sichere, vollständig verwaltete Cloud-Videoüberwachungslösung, die ein End-to-End-Videomanagementsystem mit Hardware und Software bietet, die für unübertroffene Sicherheit und Zugänglichkeit ausgelegt sind. Das Eagle Eye Cloud VMS bietet autorisierten Nutzern Zugriff auf Live- und aufgezeichnete Videos und wird zur Installation, Konfiguration und Verwaltung des Systems verwendet.

Das Eagle Eye Cloud VMS wird von Experten für physische und Cybersicherheit entwickelt und gewartet, um die CIA Ihrer Daten zu schützen. Die Software und Firmware, die die Plattform unterstützen, werden von Eagle Eye Networks verwaltet und aktualisiert. Darüber hinaus führt Eagle Eye Penetrationstests und Scans durch, um die Cybersicherheit der Plattform zu gewährleisten.

Das Eagle Eye Cloud VMS verwendet eine vor Ort installierte Appliance, um eine sichere Verbindung zwischen den Kameras und der Cloud herzustellen: die Eagle Eye Bridge oder den Eagle Eye Cloud-verwalteter Videorekorder (CMVR). Eagle Eye Bridges

EAGLE EYE ARCHITEKTUR

Abbildung 2. Eagle Eye Video Management System Architektur

und CMVRs übertragen verschlüsselte Video- und Metadaten an die Eagle Eye-Cloud Rechenzentren und isolieren die Kameras vom Internet.

Videos können vollständig in der Cloud, vollständig vor Ort oder in einem hybriden Ansatz, der beide Optionen kombiniert, gespeichert werden. Das Eagle Eye-System basiert vollständig auf einer modernen, redundanten Cloud-Architektur, die sowohl mobile als auch webbrowserbasierte Schnittstellen bietet. **Abbildung 2** zeigt die Systemarchitektur.

Das Eagle Eye Cloud VMS ersetzt herkömmliche DVRs und NVRs durch eine cybersichere, cloudbasierte Lösung:

Sichere Eagle Eye Bridges/CMVRs vor Ort:

- Eagle Eye Bridges, die Videos puffern und an die Cloud senden, führen Verschlüsselung, Videodatendeduplizierung, Bandbreitenmanagement, Bewegungsanalyse und Videokomprimierung durch.
- Eagle Eye CMVRs, die alle Bridge-Funktionen ausführen und zusätzlich Videos lokal aufzeichnen und optional zur hybriden Speicherung in die Cloud senden.

Sichere, nicht vor Ort befindliche Eagle Eye-Rechenzentrumsausrüstung (die Cloud):

- Die Anwendungsserver, Systemdaten und Videodaten der Eagle Eye Videoplattform und der Video API Platform befinden sich alle im Eagle Eye Cloud-Rechenzentrum.

EAGLE EYE BRIDGES/CMVRS

Eagle Eye Bridges und CMVRs verbinden Kameras mit dem Cloud VMS. Diese Vor-Ort-Geräte sind als „gesperrte“ Geräte ausgelegt und beseitigen die Schwachstelle einer Kamera-/Internetverbindung, indem sie die eingehende Kommunikation zu den Kameras blockieren.

Jede Bridge/CMVR verfügt über mindestens zwei Netzwerkanschlüsse: einen für das Kameranetzwerk und einen für die Verbindung zum Internet. Die Bridge/CMVR weist jeder Kamera über ihren netzwerkseitigen Anschluss per DHCP eine eindeutige Adresse zu. Es gibt keine Möglichkeit, vom Internet aus direkt auf die Kameras zuzugreifen, so dass Schwachstellen im Kamerakennwort nicht durch internetbasierte Botnet-Malware oder manuelle Remote-Hacking-Versuche ausgenutzt werden können. Ebenso können die Kameras keine Verbindung zum Internet herstellen.

Eagle Eye Bridges/CMVRs puffern Videos lokal und senden sie mit Hilfe des Eagle Eye Intelligenten Bandbreitenmanagements an die Eagle Eye-Cloud, das die Datenübertragung und Bandbreitennutzung dynamisch anpasst und Übertragungen priorisiert, um die bestehende Internetverbindung optimal zu nutzen.

PUNKT-ZU-PUNKT-VERSCHLÜSSELUNGS-DIAGRAMM

Abbildung 3. Wie Eagle Eye Networks Kundendaten schützt

EAGLE EYE CLOUD-RECHENZENTRUM

Im Zentrum des Eagle Eye-Cloud Security Camera Systems befinden sich mehrere hochsichere Rechenzentren. Diese globalen Rechenzentren werden gemeinsam als Eagle Eye Cloud-Rechenzentrum bezeichnet. Die Videos und Daten jedes Kunden werden einem Rechenzentrum zugewiesen, das der jeweiligen Region am nächsten liegt, und in dreifacher Redundanz gespeichert, um die Wahrscheinlichkeit von Unterbrechungen oder des Verlusts von Videoaufzeichnungen zu verringern.

Die Standorte der Eagle Eye-Rechenzentren verfügen über Fehlertoleranz bei Komponenten und Verbindungen. Die Redundanzen bei den Netzwerkverbindungen und Stromversorgungen sowie bei der Server-Hardware eliminieren jeden einzelnen Fehlerpunkt und maximieren die Verfügbarkeit der Hardware.

Der mehrstufige Sicherheitsansatz des Eagle Eye-Cloud-Rechenzentrums stellt sicher, dass die Videodaten für die Öffentlichkeit nicht sichtbar sind. Die Kundendaten werden im Ruhezustand mit einem eindeutigen Verschlüsselungscode für jeden Kunden verschlüsselt. Außerdem sind die Rechenzentren sowohl logisch als auch physisch vom Netzwerk des Eagle Eye-Büros getrennt.

Systemsicherheit: Verschlüsselung und Authentifizierung

Zusätzlich zu den bereits besprochenen physischen Sicherheitsfunktionen verwendet das Eagle Eye Cloud VMS mehrere Formen der Verschlüsselung und Authentifizierung, um ein Höchstmaß an CIA zu gewährleisten. Das VMS verwendet Sicherheit auf Bankniveau, um Videos von der Kamera an die Cloud und von der Cloud an den Kunden zu übertragen. Das Betriebssystem, der Webserver und die Anwendungssoftware werden kontinuierlich gewartet und automatisch mit der sichersten verfügbaren Software aktualisiert, so dass keine manuellen Sicherheitspatches durch einen Systemtechniker oder den Kunden erforderlich sind.

Eagle Eye schützt Systeme und Daten mit Authentifizierungstechnologien, die verifizierten Nutzern den Zugang erlauben und anderen verwehren. Eagle Eye gewährleistet außerdem eine sichere Verbindung durch zwei Verschlüsselungsebenen: eine für die Daten selbst und eine weitere für die Übertragung der Daten von der Eagle Eye Bridge/CMVR zum Eagle Eye Cloud-Rechenzentrum. Authentifizierte Nutzer können über eine sichere Verbindung auf entschlüsselte Videos und Daten aus dem Cloud-Rechenzentrum zugreifen.

In Abbildung 3 und **Abbildung 4** ist detailliert dargestellt, wie sowohl Videodaten als auch Datenübertragungskanäle über das Eagle Eye VMS verschlüsselt werden.

PUNKT-ZU-PUNKT-VERSCHLÜSSELUNGSTABELLE

STANDORT DER DATEN	VERSCHLÜSSELUNGSTYP	
	Datenverschlüsselung	Übertragungsverschlüsselung
1 Zwischen Kamera und Schalter	Unverschlüsselt, über eine physisch isolierte Verbindung	**Unverschlüsselte, über eine physisch isolierte Verbindung**
2 Zwischen Schalter und Eagle Eye Bridge/CMVR	Unverschlüsselt, über eine physisch isolierte Verbindung	**Unverschlüsselte, über eine physisch isolierte Verbindung**
3 Zwischen Eagle Eye Bridge/CMVR und Router	AES-256-Verschlüsselung	**TLS 1.2 (oder höher)**
4 Zwischen Router und Rechenzentrum	AES-256-Verschlüsselung	**TLS 1.2 (oder höher)**
5 Auf Servern im Rechenzentrum	AES-256-Verschlüsselung	**N/A**
6 Zwischen Rechenzentrum und Endnutzer	Unverschlüsselt	**TLS 1.2 (oder höher)**

Abbildung 4. Beschreibung der Punkt-zu-Punkt-Verschlüsselung

SICHERHEIT DER DATENÜBERTRAGUNG

Die Server des Eagle Eye Cloud-Rechenzentrums verwenden ein digitales Zertifikat, um eine sichere Verbindung zu jeder Eagle Eye Bridge/CMVR mit Transport Layer Security (TLS) 1.2 oder höher herzustellen, wodurch Datenschutz und Datenintegrität auf dreifache Weise gewährleistet werden:

1. Authentifizierung der kommunizierenden Anwendungen mit digitalen Zertifikaten.
2. Sicherstellung der privaten Verbindung durch Verwendung einer starken Datenverschlüsselung.
3. Verhindern der Änderung der Daten während der Übertragung durch eine Nachrichtenintegritätsprüfung.

Die mobile App, die Webanwendung und die APIs von Eagle verwenden ebenfalls TLS-Version 1.2 oder höher.

DATENVERSCHLÜSSELUNG

Die Privatsphäre der Videodaten wird mit der Advanced Encryption Standard (AES) 256-Bit-Verschlüsselung, dem sichersten verfügbaren Verschlüsselungsalgorithmus, sowohl auf den Eagle Eye Bridges/CMVRs als auch im Eagle Eye Cloud-Rechenzentrum geschützt. AES-256 ist die gleiche Verschlüsselungsstufe, die auch in Banken-, Regierungs- und Militäranwendungen verwendet wird.

Eagle Eye verwendet digitale Zertifikate, vergleichbar mit einem elektronischen Personalausweis, um Nutzer zu authentifizieren und den Zugriff auf ihre unverschlüsselten Videodaten zu ermöglichen.

Eine anerkannte Zertifizierungsstelle (CA) eines Drittanbieters verwaltet die digitalen Zertifikate, um Verbindungen zum Eagle Eye Cloud VMS zu authentifizieren. Dieselbe Zertifizierungsstelle wird von den wichtigsten Webbrowsern verwendet und als vertrauenswürdig eingestuft. Für Eagle Eye Bridges/CMVRs stellt Eagle Eye seine eigenen Zertifikate aus, da das Unternehmen eine vertrauenswürdige physische Verwahrkette beim Einbau der Zertifikate in die Geräte als Teil des Herstellungsprozesses garantieren kann.

NUTZERAUTHENTIFIZIERUNG

Die Endnutzer müssen von einem Administrator zum System hinzugefügt werden, bevor sie auf das VMS zugreifen können. Bei den Administratoren handelt es sich entweder um eine oder mehrere Personen innerhalb des Unternehmens, das das Konto verwaltet, oder in einigen Fällen um den Sicherheitsintegrator/Händler, der das Konto verwaltet. Die Administratoren legen den Zugriff der einzelnen Nutzer auf das System fest. Einige der Nutzerrechte sind:

- Die Möglichkeit, Live- oder aufgezeichnete Videos anzuzeigen
- Die Möglichkeit, Videos herunterzuladen
- Beschränkungen, welche Kameras oder Standorte angezeigt werden können
- Wann ein Nutzer nach Tag oder Uhrzeit auf das System zugreifen kann
- Autorisierung zum Ändern von Kameraanalysen und Einstellungen
- Zugriff auf Kontoeinstellungen oder Audit-Protokolle

Zwei verfügbare Arten der sicheren Authentifizierung schützen den Zugriff der Nutzer auf das Eagle Eye Cloud VMS über mobile Apps oder Webbrowser:

Multi-Faktor-Nutzerauthentifizierung (MFA) – Eagle Eye bietet MFA für alle Konten an, um hohe Sicherheit zu gewährleisten, indem der Systemzugriff nur von vertrauenswürdigen Geräten aus ermöglicht wird. Ein verifiziertes Gerät ist ein mobiles Gerät oder ein Browser auf einem bestimmten Computer, das zuvor mit einer dem Eagle Eye Nutzer zugeordneten Telefonnummer oder E-Mail-Adresse authentifiziert wurde. Der Nutzer erhält eine SMS oder eine E-Mail-Bestätigung, um das Gerät zu autorisieren.

Single Sign On (SSO) – Mit SSO können Systemadministratoren den Zugriff auf das Eagle Eye Cloud VMS über ihr Active Directory oder LDAP ganz einfach hinzufügen oder widerrufen, um den Zugriff für autorisierte Nutzer zu vereinfachen. Wenn sich ein Nutzer bei der SSO-Lösung anmeldet, überprüft das SSO die Anmeldeinformationen des Nutzers in einem Identitätsmanagementsystem und erstellt ein digitales Zertifikat, das seine Identität überprüft. Dieses digitale Zertifikat wird entweder im Browser oder auf dem Server des SSO gespeichert und von der Anwendung überprüft, bevor dem Nutzer Zugriff gewährt wird. SSO ist als Teil der Professional und Enterprise Editions des VMS verfügbar.

Eagle Eye bietet auch ein IP-Whitelisting, mit dem Unternehmen den Kamera- und Systemzugriff auf zugelassene Netzwerke beschränken können. Diese Funktion ist als Teil der Eagle Eye VMS Enterprise Edition verfügbar.

SCHUTZ DER KUNDENDATEN

Neben der Sicherheit und dem Schutz der Privatsphäre, die durch die fortschrittliche Verschlüsselung gewährleistet werden, sorgen zusätzliche Sicherheitsmaßnahmen dafür, dass die Videos und Daten geschützt und nur für autorisierte Nutzer zugänglich sind. Kein Kunde hat Zugriff auf das System oder die Daten eines anderen Kunden. In der Standardeinstellung hat Eagle Eye Networks keinen Zugriff auf die Video-, Daten- und Systemeinstellungen der Kunden.

Es gibt einen Mechanismus, mit dem Eagle Eye Networks Zugriff auf Kontoeinstellungen und Videos mit entsprechenden Berechtigungen erhält. Dazu gehört die Kombination aus einer erforderlichen Support-PIN und dem optionalen Datenschutzmodus.

Support-PIN: Wenn ein Nutzer unsere technische Support-Abteilung anruft, muss er eine persönliche Identifikationsnummer (PIN) angeben, die über das Kontoprofil des Nutzers verfügbar ist. Jedem neuen Nutzer wird eine anfängliche Support-PIN zugewiesen, und die Nutzer können die PIN jederzeit ändern. Die Support-PIN authentifiziert die Anmeldedaten des Anrufers, um Cyberkriminelle daran zu hindern, sich als Kunden auszugeben, und verhindert außerdem den unbefugten Zugriff auf Eagle Eye-Mitarbeiter. Die Support-PIN dient als Schlüssel zur Zugangskontrolle des Nutzerkontos. Sobald Eagle Eye Zugang hat, kann es auf Kundeneinstellungen, Kontoprotokolle und Kameras zugreifen, aber nicht unbedingt auf das Live- oder aufgezeichnete Video.

Datenschutzmodus: Der Datenschutzmodus schafft eine weitere Stufe der Videosicherheit für die Kunden. Während die Support-PIN die Einlasskontrolle für das Konto darstellt, fungiert der Datenschutzmodus als „Lichtschalter“ für das Video. Wenn der Datenschutzmodus aktiviert ist, haben Eagle Eye-Mitarbeiter keinen Zugriff auf Videos. Der Datenschutzmodus ist eine Standardfunktion, die es Eagle Eye VMS-

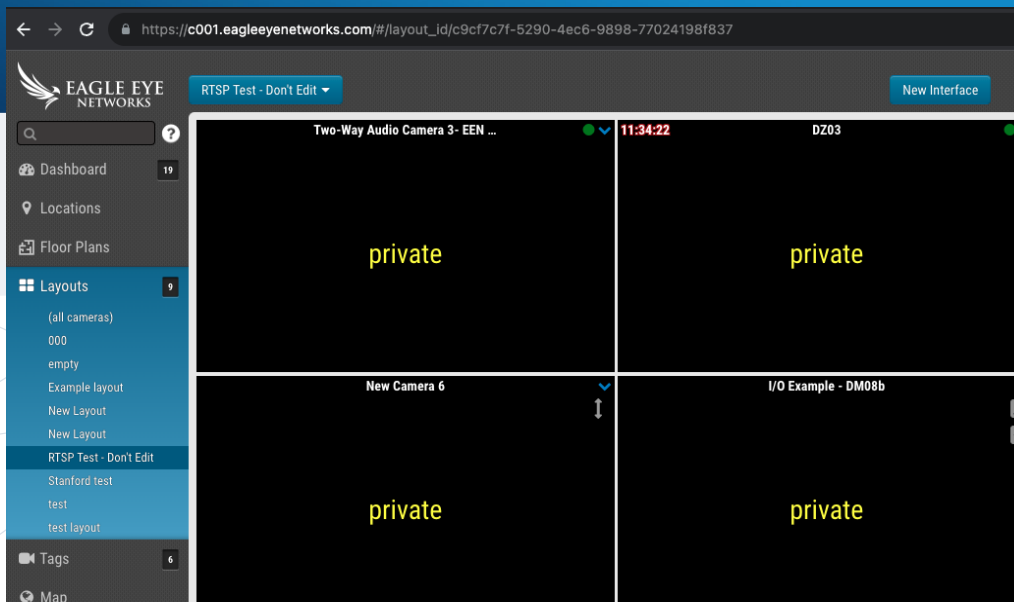

Abbildung 5. Eagle Eye Networks VMS Dashboard mit aktiviertem Datenschutzmodus.

Nutzern ermöglicht, den Zugriff auf Videostreams zu blockieren und gleichzeitig den notwendigen technischen Zugriff zu ermöglichen. Wenn der Zugriff auf den Videostream erforderlich ist (z. B. um das genaue Sichtfeld einer Kamera zu überprüfen), kann der Datenschutzmodus vom Nutzer vorübergehend deaktiviert werden.

Audit-Protokolle: Um zusätzliche Sicherheit zu bieten, verfolgen Audit-Protokolle jede Aktion im VMS von Endnutzern, Administratoren oder Eagle Eye Networks-Mitarbeitern. Audit-Protokolle werden ein Jahr lang innerhalb des Kontos gespeichert. Zu den protokollierten Aktionen gehören:

- Anmeldeinformationen
- Videoansichten und Downloads
- Änderungen an den Einstellungen

Schlussfolgerung

Das Eagle Eye Networks Cloud VMS ist eine speziell entwickelte Cloud-Videoüberwachungslösung, die das Risiko von Cybersicherheitslücken reduziert. Der stets verwaltete, abonnementbasierte Service von Eagle Eye bietet automatische System-Sicherheitsupdates, um ein Höchstmaß an Vertraulichkeit, Integrität und Verfügbarkeit von Überwachungsvideos zu gewährleisten.

So konnte Eagle Eye Networks die Risiken für die Cybersicherheit von Videoüberwachungssystemen erheblich reduzieren:

- Entwurf und Aufbau einer hochsicheren Anwendung auf der Grundlage einer modernen redundanten Cloud-Architektur
- Entwicklung eines cybersicheren cloudbasierten Überwachungskamera-Videomanagementsystems mit standardbasierter Verschlüsselung von Videodaten und -übertragungen sowie starker Authentifizierung von Nutzern und mobilen Geräten
- Herstellung speziell entwickelter sicherer Videoanwendungen, die Kameras von Internet-Bedrohungen isolieren
- Automatische Verwaltung und Aktualisierung von Sicherheits- und Funktionsupdates für die Eagle Eye-Appliance, ohne dass ein Installateur oder Endnutzer aktiv werden muss

Der stets verwaltete, abonnementbasierte Service von Eagle Eye bietet automatische System-Sicherheitsupdates, um ein Höchstmaß an Vertraulichkeit, Integrität und Verfügbarkeit von Überwachungsvideos zu gewährleisten.

Zusammenfassung der technischen Cybersicherheitsmaßnahmen

Die folgenden Listen fassen die in diesem Papier beschriebenen technischen Maßnahmen zur Cybersicherheit zusammen:

CYBERSICHERHEIT VON GERÄTEN VOR ORT

- Kameras sind vom Internet isoliert
- Die Geräte haben keine offenen eingehenden Netzwerkports
- Die Geräte sind vor vorinstallierter Kameramalware geschützt
- Die Geräte verwenden TLS 1.2-Verbindungen zum Eagle Eye-Cloud Security Camera VMS
- Die AES-256-Verschlüsselung wird auf gepufferte und lokal aufgezeichnete Videos angewendet
- Die Geräte werden über digitale Zertifikate authentifiziert

PHYSISCHE SICHERHEIT DES RECHENZENTRUMS

- Einbruchmelde- und Alarmsystem in Einrichtungen
- Zugangskontrolle für den Bereich der biometrischen Einrichtungen
- 24/7 Live- und aufgezeichnete Videoüberwachung vor Ort
- Verifizierung der Identität der Besucher des Security Desk und Besucherprotokoll

NETZWERKSICHERHEIT IM RECHENZENTRUM

- Übersetzung von Netzwerkadressen (NAT)
- Kundendaten werden im Ruhezustand mit eindeutigen Verschlüsselungscodes verschlüsselt
- Logische und physische Trennung der Rechenzentrumsumgebungen vom Eagle Eye-Unternehmensnetzwerk

REDUNDANZ

- Die VMS-Komponenten von Eagle Eye-Cloud Security Camera sind redundant (entweder aktiv/aktiv oder aktiv/passiv)
- Dreifach redundante Videodatenspeicherung, Stromversorgung und Internetkonnektivität

ANWENDUNGS- UND DATENSICHERHEIT

- Regelmäßige Scans von Server-Schwachstellen
- Regelmäßige Penetrationstests
- Sicherheit auf API-Ebene
- Multi-Faktor-Authentifizierung für den Web- und mobilen Zugriff
- TLS 1.2-Verbindungen mit Eagle Eye-Cloud Security Camera VMS für den Web- und mobilen Zugriff
- AES-256-Verschlüsselung von aufgezeichneten Videos
- Datensicherheitskontrollen für mehrere Mieter

ÜBER EAGLE EYE NETWORKS

Eagle Eye Networks, Inc. („Eagle Eye“) wurde 2012 gegründet und ist der führende globale Anbieter von cloudbasierten Videoüberwachungslösungen, welche die Bedürfnisse von Unternehmen, Alarmunternehmen, Sicherheitsintegratoren und Einzelpersonen erfüllen. Die 100 % cloudbasierten Lösungen von Eagle Eye bieten Aufzeichnungen in der Cloud und vor Ort, Sicherheit und Verschlüsselung auf Bankebene sowie umfassende Unterstützung für analoge und Digitalkameras, auf die alle über das Internet oder über mobile Anwendungen zugegriffen wird. Unternehmen aller Größen und Arten nutzen Eagle Eye-Lösungen zur betrieblichen Optimierung und Sicherheit. Alle Eagle Eye-Produkte profitieren von der entwicklerfreundlichen RESTful-API-Plattform und dem Big Data Video Framework TM von Eagle Eye, die die Indizierung, Suche, Abfrage und Analyse von Live- und archivierten Videos ermöglichen. Die offene Video-API von Eagle Eye hat sich für die Integration in die Alarmüberwachung, die Analyse von Drittanbietern, Sicherheits-Dashboards und die Integration von Kassensystemen durchgesetzt.

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

ÜBER DEAN DRAKO

Das von Dean gegründete Unternehmen Eagle Eye Networks ist das erste Cloud-basierte Videoüberwachungsunternehmen, das sowohl Cloud- als auch Vor-Ort-Aufzeichnungen anbietet.

Dean hat im Laufe seiner beeindruckenden Karriere bemerkenswerte Firmen im Bereich Sicherheit geleitet und tut dies auch weiterhin. Gleichzeitig mit Eagle Eye Networks ist Dean Eigentümer und Vorsitzender von Brivo, einem Unternehmen für Cloud-Zugangskontrolle. Zuvor hatte Dean als Gründer, Präsident und CEO von Barracuda Networks die erste E-Mail-Sicherheitsanwendung der Branche entwickelt. Bevor er zu Barracuda Networks kam, gründete Dean Boldfish, einen führenden Anbieter von Lösungen für ausgehende E-Mails in Unternehmen, der 2003 von Siebel Systems übernommen wurde. Dean war Gründer, Präsident und CEO von Design Acceleration, Inc. (DAI), einem Hersteller hochwertiger Designanalyse- und Verifikationswerkzeuge, der 1998 von Cadence Design Systems übernommen wurde.

Dean war der Gründer des Unternehmens und erhielt seinen BSEE von der University of Michigan, Ann Arbor, und seinen MSEE von der University of California, Berkeley.

Goldman Sachs kürte Dean zu einem der „100 faszinierendsten Unternehmer 2014“.

MEHR ERFAHREN
Besuchen Sie unsere Website
EEN.COM

USA
+1-512-473-0500
sales@een.com

LATEINAMERIKA/KARIBIK
+52 55 8526 4926
LATAMsales@een.com

EUROPA
+31 20 26 10 460
EMEAsales@een.com

ASIATISCH-PAZIFISCHER RAUM
+81-3-6868-5527
APACsales@een.com