EAGLE EYE NETWORKS

12 bewährte Vorgehensweisen für Überwachungskamerasysteme

Whitepaper von Dean Drako, CEO von Eagle Eye Networks

Fragen?

+31 20 26 10 460
emeasales@een.com
www.een.com

Einführung

Überwachungskamerasysteme sind - hauptsächlich aufgrund der Kundennachfrage nach Fernzugriff auf Videos - zunehmend mit dem Internet verbunden. Die Systeme reichen von in der Cloud verwalteten Überwachungssystemen über herkömmliche mit dem Internet verbundenen DVR/VMS/NVRs bis zu traditionellen Systemen in einem lokalen Netzwerk, das wiederum mit dem Internet verbunden ist.

Da Cyberangriffe immer häufiger auftreten, müssen Integratoren für physische Sicherheit und interne Supportmitarbeiter in Bezug auf die Bedrohungsvektoren für Cybersicherheit, die Auswirkungen auf die von ihnen verkauften bzw. unterstützen Kameravideomanagementsysteme haben können, auf dem neuesten Stand bleiben. Diese Systeme erfordern denselben Schutz vor Cyber-Sicherheitslücken, der für herkömmliche IT-Systeme angewendet wird.

Dieses Dokument konzentriert sich auf die Best Practices für mit dem Internet verbundene Überwachungskamerasysteme. Viele dieser Praktiken können auch bei anderen physischen Sicherheitssystemen angewendet werden.

1. Physische Sicherheit: Eine gefährliche Einfallspforte für Cyberangriffe

Überwachungskamerasysteme sind aufgrund der Nachfrage nach Fernzugriff bzw. -steuerung, Integration und drastisch gesunkenen Cloud-Speicherkosten in zunehmendem Maße mit dem Internet verbunden.

Neben der wachsenden Anzahl von in der Cloud verwalteten Überwachungssystemen sind die meisten herkömmlichen Sicherheitskamerasysteme jetzt für den Fernzugriff, den Support und die Wartung mit dem Internet verbunden oder sie sind Teil eines lokalen Netzwerks, das wiederum mit dem Internet verbunden ist.

Parallel dazu nehmen Cyberangriffe weiter zu. Über Millionen von Verstößen in den Schlagzeilen zu lesen wird alltäglich. Die Haftung für Schäden ist für Unternehmen ein großes Risiko.

Daher ist es wichtig, dass Überwachungskamerasysteme die gleiche Aufmerksamkeit und den gleichen Schutz vor Cyber-Sicherheitslücken erhalten wie herkömmliche IT-Systeme.

Integratoren für physische Sicherheit und interne Supportmitarbeiter müssen in Bezug auf die Bedrohungsvektoren für Cybersicherheit, die Auswirkungen auf die von ihnen verkauften bzw. unterstützen Kameravideomanagementsysteme haben können, auf dem neuesten Stand bleiben.

Dieses Dokument konzentriert sich auf die Best Practices für mit dem Internet verbundene Überwachungskamerasysteme. Viele dieser Praktiken können auch auf andere Überwachungskamerasysteme angewendet werden.

2. Hauptangriffsvektoren für Sicherheitskamerasysteme

Fünf große Cyber-Angriffsvektoren für Überwachungskamerasysteme sind:

1. Windows-Betriebssystem
2. Linux-Betriebssystem
3. DVRs, NVRS, VMS
4. Endpunkte (Kameras)
5. Firewall-Ports

Wir werden diese Angriffsvektoren im Zusammenhang mit anwendbaren Best Practices diskutieren, die zum Schutz Ihres Überwachungssystems gegen sie eingesetzt werden können.

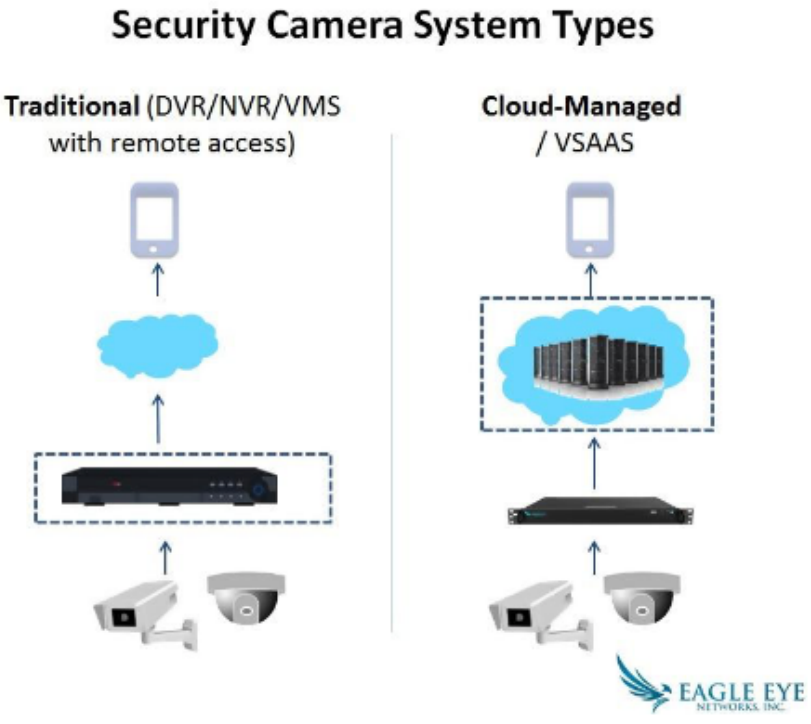
3. Best Practices unterscheiden sich je nach Typ des Überwachungssystems

Der Begriff “Cloud-Videoüberwachung” und “Cloud-System” wird uneinheitlich verwendet. Daher ist es wichtig, dass Sie sich bei Ihrem Anbieter erkundigen, wie genau er den Internetzugang bereitstellt. Dies hat nämlich Auswirkungen darauf, welche Schritte Sie unternehmen müssen, um die Sicherheit Ihres Systems zu gewährleisten.

Für die Zwecke dieses Papiers werde ich die Systemtypen wie folgt unterscheiden:

- Ein **herkömmliches System,** entweder DVR, NVR oder VMS, mit Internetverbindung, normalerweise für den Fernzugriff auf Video.
- Ein **Cloud-verwaltetes System**, auch VSAAS genannt. Bei einem in der Cloud verwalteten System wird das Video, obwohl es ein Gerät vor Ort geben mag, von der Cloud aus aufgenommen und von dort verwaltet.

In jeder dieser Kategorien gibt es Unterschiede, die sich auf Features und Funktionen auswirken. Diese Unterscheidung auf oberster Ebene bietet jedoch Klarheit darüber, wie Sie bewährte Vorgehensweisen für Cybersicherheit anwenden können und welche Fragen Sie Ihrem Anbieter stellen müssen.



4. Best Practices für Cyber-sichere Sicherheitskamerasysteme

4.1 Kamerapasswörter

Schwachstelle

Auf den ersten Blick erscheint das Passwort für die Kamera als zu offensichtlich, um besprochen zu werden. In einem Artikel von Network World im November 2014 wurde jedoch erwähnt, dass 73.011 Standorte mit IP-Kameras aus 256 Ländern auf einer Webseite veröffentlicht wurden. Die Vereinigten Staaten führten die Liste mit 11.046 Links an, wobei jeder Link bis zu 8 oder 16 Kameras enthalten konnte.

Außerdem wird geschätzt, dass jeder fünfte Webbenutzer immer noch leicht zu hackende Passwörter verwendet.

Nachstehend sind die Top 10-Passwörter für 2013 gemäß Splash Data aufgeführt.

1. 123456
2. Passwort
3. 12345678
4. qwerty
5. abc123
6. 123456789
7. 111111
8. 1234567
9. iloveyou
10. adobe123

Fast alle heute verkauften Kameras verfügen über eine webbasierte grafische Benutzeroberfläche (GUI) und werden mit einem Standardbenutzernamen und -passwort ausgeliefert, die im Internet veröffentlicht werden.

Einige Installateure ändern das Passwort überhaupt nicht und behalten bei allen Kameras dasselbe Standardpasswort.

Nur sehr wenige Kameras verfügen über eine Möglichkeit zum Deaktivieren der GUI. Daher besteht die Sicherheitslücke darin, dass jemand versuchen kann, sich über die Web-GUI in die Kamera zu hacken, um ein Passwort zu erraten.

Der Hacker muss dazu über das Netzwerk auf die Kameras zugreifen können. Die Kameras befinden sich häufig in einem gemeinsam genutzten Netzwerk, nicht in einem physisch getrennten Netzwerk oder in einem VLAN.

Best Practice:

Traditionelles System und Cloud-verwaltetes System

Es empfiehlt sich, für jede Kamera ein eindeutiges, langes, schwer zu erratendes Passwort zu vergeben. Ein solch akribischer Prozess erfordert Zeit für die Einrichtung, ist schwieriger zu verwalten und sehr schwer nachzuverfolgen. Daher verwenden viele Installateure leider ein einzelnes Passwort für alle Kameras in einem Konto.
Um dieser Herausforderung gerecht zu werden, ist eine akzeptable Best Practice:
Öffentliches Netzwerk: Für jede Kamera ein anderes sicheres Passwort
VLAN oder physisch privates Netzwerk: dasselbe sichere Passwort für alle Kameras verwenden.

Best Practice:

Traditionelles System

Verbinden Sie Ihren ungeschützten Server am besten NICHT mit dem Internet. Wenn Sie Ihr System mit dem Internet verbinden, leiten Sie so wenig Ports wie möglich „weiter“ und verwenden Sie eine moderne Firewall, die das Protokoll analysiert und inkorrekte Protokolle blockiert, die über den falschen Port gesendet werden. Stellen Sie im Idealfall auch ein IDS/IPS für erhöhten Schutz bereit.

Cloud-verwaltetes System

Die sichereren Cloud-basierten Systeme verfügen über keine Portweiterleitung, sodass keine Sicherheitslücke besteht und keine inkrementellen Schutzmaßnahmen erforderlich sind. Bitten Sie Ihren Integrator oder Anbieter, dies für jedes System zu überprüfen, das Sie besitzen oder das Sie zu erwerben gedenken.

4.2 Portweiterleitung

Schwachstelle

Die meisten Endbenutzer fordern und erwarten heutzutage Fernzugriff auf Videos von mobilen Geräten.
Diese Funktion wird normalerweise bereitgestellt, indem der DVR, NVR oder VMS auf irgendeine Weise mit dem Internet verbunden wird.
Diese typische Verbindung eines HTTP-Servers mit dem Internet ist äußerst gefährlich, da es eine Vielzahl von Möglichkeiten gibt, die für den böswilligen Zugriff verwendet werden können.
Mit dem Internet verbundene Maschinen werden normalerweise mehr als 10.000 Mal pro Tag gescannt.
Ein Beispiel für diese Sicherheitslücke war 2014 die Ausnutzung der Heartbleed OpenSSL. Viele Hersteller mussten Benutzer auffordern, ihre Passwörter zurückzusetzen.

4.3 Firewalls

Schwachstelle

Wie bereits erwähnt, sollte jeder vor Ort installierte DVR/NVR/VMS zum besseren Schutz über eine Firewall verfügen, insbesondere wenn Sie ihn über ein Fernzugriffssystem für das Internet freigeben möchten.
Firewalls können mit Tausenden von Regeln sehr komplex sein. Die modernen Firewalls sind noch komplexer, da sie die Protokolle analysieren, die über die Ports gehen, und überprüfen, ob die richtigen Protokolle verwendet werden.

Best Practice:

Traditionelles System

Am besten beauftragen Sie einen professionellen Experten für Netzwerksicherheit damit, eine moderne Firewall zu überprüfen und zu konfigurieren.
Es ist äußerst wichtig, eine klare Dokumentation der Firewall-Konfiguration zu haben und die erforderlichen Änderungen an der Firewall-Konfiguration regelmäßig zu identifizieren und zu implementieren.

Cloud-verwaltetes System

Für eine Cloud-basierte Lösung ohne Portweiterleitung ist keine Firewall-Konfiguration vor Ort erforderlich. Sprechen Sie mit Ihrem Integrator oder Systemhersteller, um dies zu bestätigen.

4.4 Netzwerktopologie

Schwachstelle

Das Mischen der Kameras in einem Standardnetzwerk ohne Trennung führt mit Sicherheit zu einer Katastrophe.
Wenn Ihr Sicherheitskamerasystem mit Ihrem Hauptnetzwerk verbunden ist, öffnen Sie eine Tür für Hacker, die über Ihr Überwachungssystem in Ihr Hauptnetzwerk oder über Ihr Hauptnetzwerk in Ihr physisches Sicherheitssystem gelangen können.
Einige DVRs sind sogar bereits bei Versand mit einem Virus infiziert.

Best Practice:

Traditionelles System und Cloud-verwaltetes System

Ideales Best Practice:
Platzieren Sie das Sicherheitskamerasystem idealerweise in einem Netzwerk, das physisch vom Rest Ihres Netzwerks getrennt ist.

Akzeptable Best Practice:
Wenn Sie mit einer hoch entwickelten IT-Umgebung integrieren, ist es nicht immer möglich, die beiden Systeme physisch zu trennen.

In diesem Fall sollten Sie ein VLAN verwenden.

4.5 Betriebssysteme

Schwachstelle

Ihr VMS, DVR, NVR oder Aufzeichnungssystem vor Ort verfügt über ein Betriebssystem. Die Kameras verfügen alle über ein Betriebssystem.
Alle Betriebssysteme, sowohl Windows- als auch Linux-basierte Systeme, weisen Sicherheitslücken auf.
Windows-Sicherheitslücken sind so weit akzeptiert, dass IT-Teams sie regelmäßig überwachen. In letzter Zeit wurde immer deutlicher, dass Linux auch viele Schwachstellen aufweist, wie beispielsweise Shellshock (2014) und Ghost (2015), die Millionen von Systemen anfällig machten.
Theoretisch verfügt Ihr Systemhersteller über ein hochqualitatives Sicherheitsteam, das Sie rechtzeitig mit Sicherheitsupdates versorgt. Die Realität ist, dass viele Anbieter dies nicht auf einer verlässlichen Basis tun.

Best Practice:

Traditionelles System

Um sicherzustellen, dass Ihr System und Ihr Netzwerk vor bösartigen Angriffen geschützt sind, sollten Sie bekannte Schwachstellen des Betriebssystems beobachten und überwachen und dann sicherstellen, dass alle Sicherheits-Patches für Ihr Betriebssystem auf dem neuesten Stand sind.

Wenn es sich um ein Windows-basiertes System handelt, gibt es viele Schwachstellen und zahlreiche Updates müssen installiert werden. Auch wenn Linux-Schwachstellen weniger häufig auftreten, müssen sie schnell verfolgt und behoben werden.

IT-Sicherheitsexperten verstehen normalerweise, welche relevant sind und welche Sie überspringen können. Dies kann jedoch ohne entsprechende Schulungen und Erfahrung eine äußerst schwierige Aufgabe sein.

Sie können sich auch proaktiv an Ihren DVR-/NVR-Hersteller wenden, um herauszufinden, welches Betriebssystem Ihr NVR/DVR verwendet (Linux, Windows) sowie die Betriebssystemversionen und die Versionen der zusätzlichen Module, die auf dem Betriebssystem aufsetzen (z. B. Microsoft IIS-Webseitenserver).
So können Sie verstehen, von welchen Sicherheitslücken Sie betroffen sind. Identifizieren Sie dann die Schwachstellen dieses Betriebssystems und wenden Sie sich an Ihren Betriebssystemanbieter, um zu erfahren, welche Patches erforderlich sind.

Die bewährten Verfahren für ein VMS bestehen darin, sicherzustellen, dass sich die Maschinen in der Verantwortung der IT-Abteilung befinden und dass die IT-Abteilung die Verantwortlichkeiten zugewiesen und das Personal für das richtige Patchen, Aktualisieren, Modifizieren hat, und Prozesse bestehen, um die Sicherheit der Maschinen zu

gewährleisten.

Stellen Sie außerdem sicher, dass Ihr Kamerahersteller Sicherheitspatches zur Verfügung stellt, und dass Sie Ihre Kamera-Firmware aktualisieren, sobald neue Versionen verfügbar sind.

Cloud-verwaltetes System

In diesem Fall sollten Sie sich bei Ihrem Integrator oder Cloud-Anbieter erkundigen, ob der Cloud-Anbieter über ein dezidiertes, erfahrenes Sicherheitsteam verfügt, das Schwachstellen überwacht.
Vergewissern Sie sich außerdem, dass der Cloud-Anbieter Sicherheitspatches/-Updates automatisch über die Cloud an die Installationen vor Ort sendet. In diesem Fall ist vom Endbenutzer keine Aktion in Bezug auf die Sicherheitsüberwachung, das Patchen oder das Upgrade des Betriebssystems erforderlich.

4.6 Betriebssystemkennwörter

Schwachstelle

Wie bei Kamerapasswörtern kann ein schwaches Systempasswort die Tür für Cyberangriffe auf das Überwachungssystem und das Netzwerk öffnen. In vielen Betriebssystemumgebungen wird das Root-Passwort oder das Administratorpasswort von allen Administratoren gemeinsam genutzt, wodurch das Sicherheitsrisiko erhöht wird.

Die Fluktuation der Mitarbeiter, entweder durch Kündigungen oder durch Rollenwechsel, kann zu unerwarteten Sicherheitslücken führen.

Best Practice:

Traditionelles System

Legen Sie hochwertige lange Passwörter für das Betriebssystem fest.

Richten Sie außerdem Richtlinien und Verfahren zum Ändern von Passwörtern ein. Beispielsweise sollte das Root-Administratorpasswort jedes Mal geändert werden, wenn ein Mitarbeiter mit Passwortzugang das Unternehmen verlässt oder seine Rolle sich ändert.

Cloud-verwaltetes System

Keine Aktion erforderlich. Echte Cloud-Systeme haben keine separaten Passwörter für den Zugriff auf das Betriebssystem. Sie haben nur Systempasswörter für einzelne Konten (siehe unten), die explizit gelöscht werden, wenn Mitarbeiter ausscheiden oder in eine andere Rolle wechseln.

4.7 Systempasswörter

Schwachstelle

Unbefugter Zugriff auf Ihr Sicherheitskamerasystem macht sowohl das Überwachungssystem anfällig als auch das damit verbundene Netzwerk.

Best Practice:

Traditionelles System und Cloud-verwaltetes System

Ändern Sie die Passwörter Ihres Überwachungssystems nach einem Zeitplan. Setzen Sie die Sicherheitsqualität mit der gleichen Strenge durch wie Ihren Unternehmensstandard. Lange, starke Passwörter sind die besten.

4.8 Anschlusstechnik

Schwachstelle

Eine überraschend große Anzahl von DVR/NVR/VMS verwendet Verbindungen, die nicht mit SSL oder auf ähnliche Weise verschlüsselt sind.
Das dadurch entstehende Risiko ist identisch mit dem Anmelden bei einer Online-Bank oder dem Online-Einkauf ohne https. Es führt zu Sicherheitslücken in Passwörtern und ermöglicht potenzielle Datenschutz- und Lauschangriffe.

Best Practice:

Traditionelles System

Es ist zwingend erforderlich, dass die Verbindung mit SSL oder auf ähnliche Weise verschlüsselt wird.
Fragen Sie Ihren Anbieter, wie er die Thematik adressiert. Wählen Sie nur Anbieter aus, die ihre Verbindungen verschlüsseln.

Cloud-verwaltetes System

Es ist zwingend erforderlich, dass die Verbindung mit SSL oder auf ähnliche Weise verschlüsselt wird.
Viele Cloud-Anbieter bieten Verbindungsverschlüsselung an, dies ist jedoch variabel. Bestätigen Sie mit Ihrem Cloud-Anbieter, wie sein System dies adressiert.

4.9 Videoverschlüsselung

Schwachstelle

Abgesehen von unsicheren Verbindungen aufgrund fehlender Verschlüsselung gelten dieselben Datenschutzrisiken, wenn das Video bei Speicherung auf der Festplatte oder während der Übertragung nicht verschlüsselt wird.

Best Practice:

Traditionelles System und Cloud-verwaltetes System

Für ein wirklich sicheres System sollten Videos verschlüsselt werden, sowohl wenn sie auf der Festplatte gespeichert werden als auch während der Übertragung.

4.10 Mobiler Zugriff

Schwachstelle

Sicherheitslücken in Bezug auf Kennwort, Kontolöschung und Verschlüsselung gelten doppelt für mobile Geräte.

Best Practice:

Traditionelles System und Cloud-verwaltetes System

Stellen Sie sicher, dass Sie eine verschlüsselte Verbindung von der mobilen Anwendung auf dem iPhone oder Android zum VMS oder NVR/DVR haben, genauso wie wenn Sie die Anwendung auf Ihrem PC ausführen.
Legen Sie hochwertige Passwörter fest und bestehen Sie bei Mitarbeiterwechsel auf Ausführung der Passwortänderungen und Löschung der Konten.

4.11 Physischer Zugang zu Ausrüstung und Lagerung

Schwachstelle

Die finanziellen Belohnungen für den Diebstahl von Unternehmensdaten sind ausreichend hoch, so dass Eindringlinge auch versuchen werden, auf Ihr Netzwerk zuzugreifen, indem sie direkt in Ihre physischen Geräte vor Ort hacken.

Best Practice:

Traditionelles System

Halten Sie unter Verschluss: Ihre Schränke; die Kabel; und den Raum, in dem sich die DVR/NVR/VMS, Switches und Videospeicherserver befinden. Sorgen Sie für eine sichere Zugangskontrolle zum Raum, einschließlich Videoüberwachung. Diese Vorgehensweise schützt nicht nur Ihr Netzwerk, sondern verhindert auch Diebstahl in Ihren Gebäuden, bei dem der aufnehmende DVR/NVR zusammen mit anderen Gegenständen gestohlen wird.

Cloud-verwaltetes System

Obwohl das gleiche Prinzip ganz klar auch für ein Cloud-basiertes System gilt, gibt es hier deutlich weniger Geräte vor Ort, die geschützt werden müssen. Die sofortige Aufzeichnung in der Cloud schützt außerdem vor Diebstahl der Aufnahmen vor Ort.

Erkundigen Sie sich bei Ihrem Integrator oder Anbieter, welche allgemeinen Sicherheitsmaßnahmen für Ihre Cloud-Server ergriffen werden.

4.12 Videoaufzeichnungssoftware

Schwachstelle

Videomanagement-Software verwendet eine Vielzahl von Komponenten außerhalb des Betriebssystems, z. B. Microsoft-Datenbankanwendungen. Wie das Betriebssystem selbst müssen auch Upgrades für diese Komponenten ausgeführt werden, um sie sicher zu halten.

Viele VMS verwenden zum Beispiel Microsoft Access oder Bibliotheken sowie die von ihnen geschriebene Software. Neue Systemschwachstellen können eingeführt werden, wenn die unterstützende Software nicht auf dem neuesten Stand, einschließlich Sicherheitspatches, ist.

Wenn Sie hier passiv sind, sind Sie in hohem Maße davon abhängig, dass der Anbieter Patches sendet, um das System gegen solche Sicherheitslücken zu aktualisieren.

Best Practice:

Traditionelles System

Erkundigen Sie sich bei Ihrem VMS-Anbieter nach seinen Richtlinien, um die von ihm verwendeten Komponenten auf dem neuesten Stand und sicher zu halten. Suchen Sie nach regelmäßigen Updates und installieren Sie diese. Seien Sie proaktiv bei der Überwachung der bekannten Sicherheitslücken in der Branche und wenden Sie sich an Ihren Integrator oder Anbieter, wenn Sie von neuen Verstößen erfahren.
Es ist wichtig sicherzustellen, dass der VMS-Anbieter über ein Team verfügt, das sich darauf konzentriert und Ihnen regelmäßig Updates sendet.

Cloud-verwaltetes System

Echte Cloud-verwaltete Systeme verfügen über keine Software vor Ort. Daher besteht hier keine Sicherheitslücke.
Es ist jedoch sehr wichtig, zu überprüfen, ob das System wirklich “Cloud-verwaltet” oder mit dem Internet verbunden ist, bevor Sie diese Annahme treffen. Ansonsten riskieren Sie, einer potenziellen Schwachstelle ausgesetzt zu sein.

Fazit

Datenschutzverletzungen nehmen weltweit immer mehr zu. Mit zunehmender Internet-Konnektivität sind physische Sicherheitssysteme sehr anfällig für Cyber-Angriffe, sowohl in Bezug auf direkte Angriffe als auch als Zugangstor zum Rest des Netzwerks. Die Haftungsfragen für diese Angriffe werden noch diskutiert.

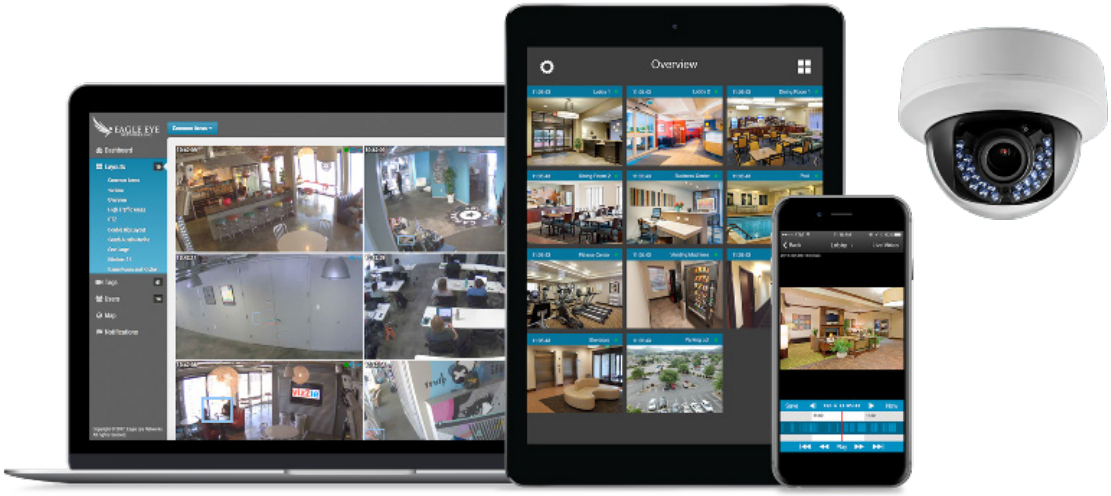
Es ist ratsam, Ihr Unternehmen und Ihre Kunden durch vorbeugende Maßnahmen zu schützen. Um Ihre Cyber-Sicherheit zu maximieren, ist es entscheidend, Best Practices für Ihr eigenes Unternehmen im Rahmen der Evaluierung Ihres Sicherheitskamerasystems sowie bei seiner Bereitstellung und Wartung zu definieren.

WOLLEN SIE IHRE BUSINESS SOFTWARE AUCH IN DIE CLOUD VERLEGEN?

Erfahren Sie mehr über das Video Management System (VMS) von Eagle Eye Networks.

Eagle Eye Networks wurde geschaffen, um die Videosicherheit zu vereinfachen. Kamerasysteme waren traditionell komplex und schwierig zu verwalten. Mit der Eagle Eye Networks Cloud-VMS können Sie mehrere Kameras an mehreren Standorten bereitstellen, ohne eine Software zu installieren oder große Server erwerben zu müssen.

Erfahren Sie mehr über unser Cloud-VMS, erkunden Sie die Plattform, oder sprechen Sie heute noch mit einem unserer Spezialisten.



Eagle Eye Networks EMEA
Hogehilweg 19
1101 CB Amsterdam
The Netherlands

KONTAKTIEREN SIE UNS
+31 20 26 10 460
EMEAsales@een.com
www.een.com

Support Desk
+31 20 26 10 461
support@een.com
www.een.com/support