Kamera-Cyber-Sperrfunktion

Whitepaper von Dean Drako, CEO von Eagle Eye Networks

AUTHORIZED PARTNER

Fragen?

+ 49 (0) 251 6744 43-0
info@isn-videocloud.de
www.isn-videocloud.de

ÜBERSICHT

Die Kamera-Cyber-Sperrfunktion von Eagle Eye besteht aus einer Reihe von Cybersicherheitsfunktionen, die als Teil des Cloudsicherheitskamera-Video-Managementsystems (VMS) von Eagle Eye veröffentlicht wurden. Der Zweck der Kamera-Cyber-Sperrfunktion von Eagle Eye besteht darin, die Auswirkungen von Cybersicherheitsproblemen für Kameras deutlich zu reduzieren oder zu beseitigen.

Der Schutz von mit dem Netzwerk verbundenen Videoüberwachungskameras ist wichtig, da viele Kameras mehrere Cybersicherheitsprobleme haben:

1. Kameras werden von vielen Unternehmen auf der ganzen Welt hergestellt. Viele dieser Unternehmen haben unbekannte politische und staatliche Verbindungen.

2. Viele Kameras werden von einer Firma hergestellt, dann von verschiedenen Firmen mit ihrer Markenidentität versehen und verkauft. Es kann schwierig sein, Hersteller und Herkunftsland zu bestimmen.

3. Viele Kameradistributoren und -hersteller sind bei der Cybersicherheit zu nachlässig. Sie führen keine angemessenen Tests ihrer Kameras durch und verfügen nicht über das erforderliche Wissen, um ihre Kameras wirklich cyber-sicher zu machen. Bei der Auswahl der Kameras ist es schwierig, Cybersicherheitsprofile für die Kamera festzulegen.

4. Hersteller können versehentlich oder gewollt einen geheimen “Backdoor” -Zugang zu Kameras offenlassen.

5. Viele Kamerahersteller reagieren nicht rechtzeitig durch Firmware-Aktualisierungen, die die Sicherheitsprobleme beheben, auf die Entdeckung von Cybersicherheitslücken bei Kameras. Einige bieten überhaupt keine Firmware-Aktualisierungen an.

6. Häufig werden die veröffentlichten werkseitigen Standardkennwörter bei der Installation von Kameras nicht geändert, oder es werden leicht zu erratende Kennwörter verwendet, sodass die Kameras für Angriffe durch einzelne Hacker und automatisierte Angriffe auf das Netzwerk anfällig sind.

7. Passwörter werden oft im Klartext übermittelt und sind somit ermittelbar.

8. Das Aktualisieren der Firmware einer großen Anzahl von Überwachungskameras ist im Allgemeinen arbeitsintensiv und kostspielig.

9. Viele Kunden von Überwachungskameras (Endbenutzer) verfügen nicht über Prozesse, um die Entdeckung von Cyberschwachstellen von Kameras zu überwachen und Firmware-Aktualisierungen bei ihrer Veröffentlichung durchzuführen. Ihre Kameras bleiben anfällig.

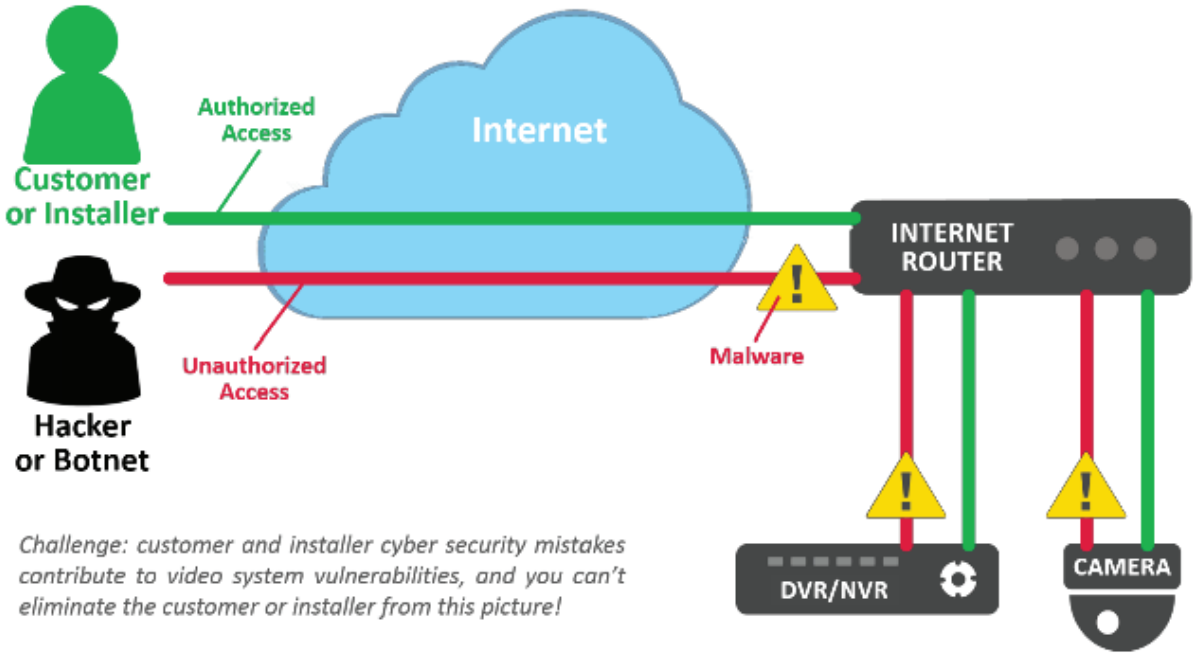
DAS PROBLEM

Teil 1: Internetverbindungen

Ein “Bot”, kurz für Roboter, ist ein Softwareprogramm, das automatisierte Aufgaben ausführt. Ein Bot-Netz ist ein Netzwerk von Computern, auf denen jeweils ein oder mehrere Bots ausgeführt werden. Hacker haben den Begriff „Bot-Netz“ verwendet, um ein Netzwerk von mit dem Internet verbundenen Geräten, einschließlich PCs, Servern, Mobilgeräten und Geräten für das Internet der Dinge, die infiziert sind und von einer verbreiteten Malware kontrolliert werden, wobei die Gerätebesitzer normalerweise keine Kenntnis von der Malware-Infektion haben, zu bezeichnen. Über das Internet verbundene Sicherheitsvideokameras und -rekorder sind zu einem bevorzugten Ziel für Infektionen durch ein Hacker-Bot-Netz geworden.

Im September und Oktober 2016 wurden die beiden größten globalen Bot-Netz-Angriffe mit mehreren hunderttausend infizierten Kameras, digitalen Videorecordern (DVRs) und Netzwerkvideorecordern (NVRs) durchgeführt. Forscher haben berichtet, dass im Jahr 2016 etwa eine Million mit dem Internet verbundene Videokameras und DVRs durch Malware infiziert wurden. Die meisten Kamera- und DVR-Besitzer wissen nicht, dass ihre Geräte infiziert sind.

Die Wurzel des Problems ist der Wunsch von Einzelpersonen und Unternehmen, Sicherheitsvideos über einen Desktop- oder Laptop-Computer, ein Tablet oder ein Smartphone aus der Ferne anzusehen. Herkömmliche DVRs und NVRs erfordern eine Verbindung AUS dem Internet zu den Rekordern (siehe rote Linien in der Abbildung unten).



Challenge: customer and installer cyber security mistakes contribute to video system vulnerabilities, and you can't eliminate the customer or installer from this picture!

Wenn der Rekorder nicht über eine Internetverbindung verfügt, können Videos nur am Standort des Rekorders angezeigt werden. Nur wenige Kunden akzeptieren diese Einschränkung auf lokale Wiedergabe.

Kameras, DVRs und NVRs bieten kaum oder gar keinen Schutz vor Cyber-Angriffen. Nur sehr wenige verfügen über integrierte Firewalls. Die meisten wurden von ihren Herstellern oder Installateuren keinen angemessenen Cyber-Sicherheitstests unterzogen. Die meisten haben große Passwort-Sicherheitslücken. Nur wenige erhalten adäquate Firmware-Aktualisierungen, um Sicherheitslücken zu beheben, und nur bei wenigen werden Betriebssystem (OS)-Lücken geschlossen, sobald Updates veröffentlicht werden.

Im Juli 2017 entdeckten Cyber-Security-Forscher einen schwerwiegenden Fehler, den sie “Devil’s Ivy” nannten, und zwar in fast allen Kameras, die die beliebte ONVIF-Spezifikation unterstützen. Der Fehler ermöglicht es Hackern, ONVIF-kompatible Kameras vollständig zu kontrollieren. Die meisten Kameramarken und -modelle sind anfällig, einschließlich hochwertiger Kameras. Innerhalb weniger Tage haben einige große Hersteller Firmware-Updates herausgegeben, die den Fehler beheben. Es liegt an den Kamerabesitzeren und Wartungsunternehmen, die Kameras zu aktualisieren. Es ist nicht abzusehen, welche Hersteller Firmware-Korrekturen für ihre Kameras vornehmen oder wie viele Millionen anfälliger installierter Kameras tatsächlich aktualisiert werden.
Wenn gefährdete Kameras und Rekorder direkt aus dem Internet angesprochen werden können, können sie von Cyberkriminellen und anderen Angreifern leicht angegriffen und ausgenutzt werden.

Teil 2: Trojaner, Spyware und vorinstallierte Viren

Es besteht ein erhebliches Problem, dass Kameras, DVRs und NVRs vom Hersteller oder vom Installateur mit bereits installierten Spyware-Programmen, Trojanern oder Viren bereitgestellt werden. Es gibt viele dokumentierte Fälle, die dies belegen.

In diesem Fall führt das Gerät eine Software aus, die entweder sofort oder zu einem vorher festgelegten Zeitpunkt versucht, einen “Command and Control Server” (CCS) im Internet zu kontaktieren, um zusätzlichen Softwarecode und Anweisungen abzurufen. Beispielsweise könnte eine gefährdete Kamera einen Trojaner haben, der versucht, sich am 15. Januar 2019 mit seinem CCS in Verbindung zu setzen. An diesem Datum verwendet die Kamera die Internetverbindung, um Anweisungen vom Server zu erhalten.

Die meisten Netzwerke erlauben ausgehende Verbindungen von jedem Gerät im Netzwerk. Komplexere Netzwerkkonfigurationen, die VLANS oder Firewalls verwenden, versuchen, ausgehende Verbindungen zu blockieren. Dies ist jedoch nicht die Norm. In einem typischen Netzwerk sind verschlüsselte ausgehende Verbindungen zu einem CCS zulässig. Dateien von Computern in einem lokalen Netzwerk, Videobilder und Passwörter können von einer infizierten Kamera leicht an Hacker übertragen werden. Die Kamera könnte dann Anweisungen und zusätzliche Software erhalten, die ausgeführt werden soll, um sich in andere Computer im Netzwerk zu hacken, Datenbanken anzugreifen, Kreditkarteninformationen zu übertragen oder an einem Denial-of-Service-Angriff (DDoS) teilzunehmen.

Bei einem Trojaner oder vorinstalliertem Virus auf einer Kamera, einem NVR oder DVR benötigt das infizierte Gerät einfach einen beliebigen Zugang zum Internet, um Teil eines Bot-Netzes zu werden und eine ernsthafte Bedrohung für die Systeme zu sein, auf die der kontrollierende Hacker abzielt.

Warum Hacker angreifen

Die Zeit, in der Kinder Webseiten nur zum Spaß hackten, ist lange vorbei. Hacken ist heute ein großes Geschäft, das Informationen stiehlt, um sie zu verkaufen, und Verschlüsselung verwendet, um von Webseiten Lösegeld zu verlangen. Diese Webseiten können beliebiger Art sein, einschließlich öffentlich zugänglicher Webseiten, Spielesysteme, E-Commerce-Webseiten und in einigen Fällen sogar Regierungssysteme.

Zu den wichtigsten Hacker-Zielen gehören:

1. Vertrauliche persönliche Informationen wie Kreditkartennummern, Sozialversicherungsnummern und andere persönliche Identifikationsinformationen (PII) zu erhalten.
2. Vertrauliche, unternehmensbezogene Informationen wie Kundendaten, Finanzberichte usw. zu erhalten.
3. Eine Webseite oder ein Netzwerk über einen verteilten Denial-of-Service-Angriff (DDoS) aus dem Verkehr zu ziehen, indem ein Bot-Netz aus Zehntausenden oder Hunderttausenden kompromittierter Geräte (oft global verteilt) verwendet wird.

DDoS-Angriffe sind die am weitesten verbreitete Art von Angriffen, die im letzten Jahr sowohl in Bezug auf Anzahl als auch Volumen stark zugenommen haben. Netzwerkkameras, DVRs und NVRs sind ideale Ziele. Ihre Schwachstellen führen zu einem höchst unsicheren System, das einfach ausgenutzt werden kann.

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.

ISN Technologies AG
Johann-Krane-Weg 46
48149 Münster
Deutschland

KONTAKTIEREN SIE UNS
+49 (0) 251 6744 43-0
info@isn-videocloud.de
www.isn-videocloud.de

AUTHORIZED PARTNER