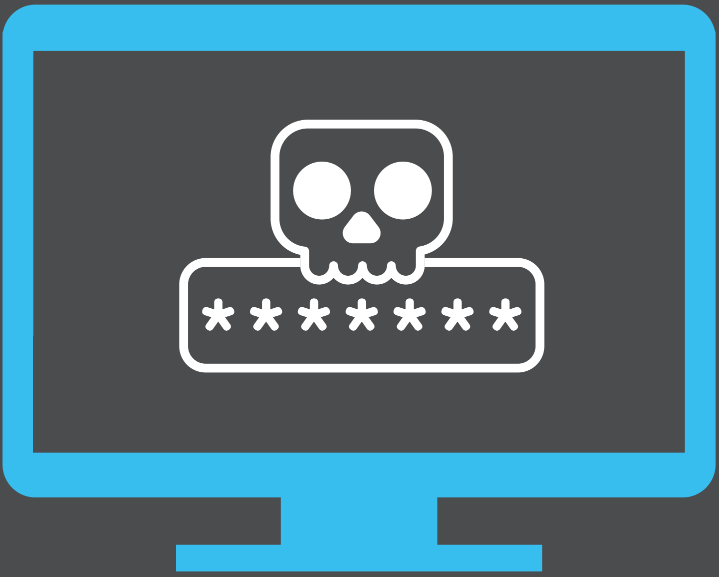
Cloudview®

Is your CCTV system secure from CYBER ATTACK?



A Cloudview White Paper

Table of contents

Executive summary

Across society, visual surveillance plays a vital role in the protection of people, property and assets. But traditional DVR-based CCTV systems leave companies vulnerable to attack from malevolent intruders. Cyber-attackers can exploit weaknesses in DVR security, find vulnerable devices and hijack connections to the device's IP address.

The failure of manufacturers to automate firmware updates also leaves DVR systems vulnerable, with little oversight or control over access and data exfiltration. In the case of an attack, a DVR acts as a gateway to a company's wider network, giving an attacker the means for undetectable corruption or the extraction of huge amounts of data.

Unfortunately, most cloud-based video solutions are just as vulnerable as traditional DVR systems. They often use the same IP connection and 'port forwarding' techniques as an old-fashioned DVR, leaving data equally insecure. A survey conducted by Cloudview of 24 cloud-video providers exposed many common security errors that left client data vulnerable. These vulnerabilities included a lack of encryption, poor cookie security, insecure user and credential management and the failure to use effective security protocols.

The majority of both DVR and cloud-based systems also failed to offer effective access and storage controls. Not only does this pose a risk to people and property, it also leaves companies on the wrong side of the law.

"The only provider currently offering the security features necessary to safeguard sensitive visual data is Cloudview."

The only provider currently offering the security features necessary to safeguard sensitive visual data is Cloudview. Using a secure, single-direction connection, from the network adapter to the cloud, Cloudview is protected from external interference; once off the premises, the data is secured by end-to-end encryption and digital signatures. Cloudview's flexible log-in and storage controls maintain access security, while enabling operators to adhere to increasingly strict Data Protection regulations.

© Cloudview (UK) Limited 2016

Introduction

Visual surveillance is more integral to society than ever before, helping organisations to safeguard their most valuable assets. However, the DVR systems traditionally employed in CCTV networks can make those very organisations vulnerable. This paper will explore the ways in which even well-known DVR systems are exposed to external cyber-attack, often acting as a potential entry point for wider corruption or extraction of network information. The paper will then examine the vulnerabilities posed by newer, cloud-based video solutions, and outline the impact that these security issues have on compliance with data protection laws.

Insecurity of DVRs

Port forwarding

Many DVRs allow users to view live or recorded footage remotely using a web browser or app, typically using 'port forwarding' to enable this functionality.

At the heart of most organisations' security protocols is their firewall. This works by preventing all inbound connections to a device, so there is no way for the DVR to form a direct connection to the internet. To get around this and enable port forwarding, a hole is punched in the firewall, and connections are forwarded to the DVR. The browser or app can now reach through the firewall and access the DVR, allowing users to connect remotely. However, with an open hole in the security perimeter, anyone can get in. The security of the network is now entirely compromised by the DVR.

> "With an open hole in the security perimeter, anyone can get in. The security of the network is now entirely compromised by the DVR."

A number of DVRs automatically set up port forwarding rules without notifying the user. The DVR simply asks the router to set up port forwarding. This makes set-up easier, but at the expense of weakened security.

Some DVRs recommend running on a non-standard port. Although this may reduce the number of automated attacks, it does make finding vulnerable DVRs easier. To mitigate this risk, a firewall can be configured to only allow certain external IPs (known as IP white-listing) to use a port forwarding rule. But even with IP white-listing, companies are still vulnerable to attack.

Finding vulnerable devices

Everything connected to the internet is identified by an IP address. So when using port forwarding to access the DVR, its IP address needs to be known. As a result, many manufacturers recommend using Dynamic DNS, which automatically updates a name server in the Domain Name Server (DNS).

However, Dynamic DNS also allows an attacker to quickly find hundreds, or even thousands of vulnerable devices relatively easily. They simply need to test as many

© Cloudview (UK) Limited 2016

names as possible until they get a response; an IP address will only be returned when there is a valid domain. In the case of specifically targeting DVRs, an attacker does not need to scour the entire internet but need only search the domains used by known brands. For example, Swann operate swanndvr.net, Hikvision operate hiddns.com and Dahua operate dahuaddns.com.

To test this theory, an independent consultant tested a list of 50,000 potential names against swanndvr.net (e.g. XXX.swanndvr.net where XXX was replaced with names). Within just a few minutes this yielded 2,400 valid domain names — i.e. 5% of the total were valid. Of those 335 (about 14%) were running an open service of some kind. At this stage, an attacker could start trying to login using default usernames and passwords, which would almost certainly gain access to a few DVRs.

In addition to the risks of Dynamic DNS, many DVRs also run on distinctive ports. For example, nearly all Dahua DVRs open port 37777, so an attacker looking for DVRs knows exactly where to look. Scanning the entire Internet for this port takes mere days, and found almost 500,000 devices which can then be subjected to attacks.

Firmware updates

Nowadays, everyone is familiar with companies releasing software updates. When a bug or vulnerability is found, the software company will develop a fix and deploy it to users, often using an automated mechanism.

However, automatic DVR firmware updates are almost unheard of. For a large number of devices, there may only be a couple of firmware updates to fix the most serious of bugs. Once the DVR is a few months old, and of no commercial interest to the manufacturer, updates generally cease, leaving companies vulnerable to attack.

Even when manufacturers do update the firmware, it is often only a small subset of the entire system. This means that they update the programs developed to handle the DVR functionality, but not the underlying operating system. An analogy would be running an up-to-date web browser on a Windows 95 machine. The browser may be secure, but the underlying operating system is so riddled with holes that it does not matter. You have locked the door, but left the windows wide open.

> "Once the DVR is a few months old, and of no commercial interest to the manufacturer, updates generally cease, leaving companies vulnerable to attack."

To highlight the extent to which DVRs are specifically targeted by attackers — and why regular security updates are necessary — the independent consultant carried out another experiment. Five routers, DVRs and IP cameras were placed onto the open internet. They were running the latest available firmware, in their default configuration. Within minutes, attackers had begun attempting to use common logins; one device fell to this most basic of intrusions. Within a few hours, each device had been port-scanned. Some were very brief scans, looking for the most obvious open services such as web servers (port 80), telnet (port 23) and FTP (port 21). However, a couple of scans focused on common DVR ports — 2000, 4000, 9000, 18700, 34567 and 37777.

© Cloudview (UK) Limited 2016

Within 24 hours, two of the devices had been entirely compromised and were under the control of an unknown attacker. The attacker was free to access the network the device was connected to, install their own software, and transfer data back out. Another device was left in an unstable state after an attempted attack, rendering it inoperable. If this was your critical CCTV system, you would have lost all surveillance.

No oversight

Generally, the first signs of a malware infection on a PC are unwanted pop-ups, a general slow-down, continuous network and disk activity, strangely-named processes or alerts from anti-virus software. Now imagine that the PC is rarely used, and when it is used, it runs a cut-down user interface with no anti-virus software. How can problems be detected? The simple answer is that they can't.

The same issues exist with a DVR. It will rarely be used; live footage might be looked at now and then, and recorded footage even less frequently. The user interface provides no feedback as to what is going on inside.

Vulnerabilities are common

> "In over 15 DVRs tested by an independent consultant, none was free from serious vulnerabilities. Some took many hours to breach, but the majority took less than an hour."

Any complex system will have some vulnerabilities, whether obvious or very subtle. Unfortunately, the majority of DVR software is not built by highly-skilled developers. Many manufacturers only require that the software works immediately. Often, the mistakes are avoidable: common errors such as unbounded memory access, SQL injection, and default credentials. Security, then, is often an afterthought. Consequently, many systems acquire security features as and when their weak points are uncovered by third parties.

Further to this, mistakes are often made at the specification stage, even before a developer has written a line of code. Manufacturers still have a predisposition to include 'back door' vulnerabilities. In over 15 DVRs tested by an independent consultant, none was free from serious vulnerabilities. Some took many hours to breach, but the majority took less than an hour. Without the ability to update firmware, backdoor vulnerability can persist for years, leaving businesses' entire network exposed.

Powerful machines

Inside a DVR is a powerful and highly capable computer, normally running a full operating system. There is little difference between a DVR and a small web server; this makes DVRs ideal machines for launching an attack against your network. In comparison, a router or internet-connected thermostat is far more limited, while many IoT devices have slow network connections, limited processing power and very little storage space.

This ability of a DVR to be used to launch an attack against the rest of a network makes the use of a cloud-based system even more compelling. This will be discussed later in this paper.

© Cloudview (UK) Limited 2016

Data exfiltration

By their nature, DVRs carry lots of network traffic in both directions — but how can companies tell what that traffic is and where it is going? Combined with their large hard drives, this makes DVRs the ideal point to extract vast quantities of data from a network.

Insecurity of cloud video solutions

Cloud video solutions are a newer breed of video surveillance systems which are beginning to replace traditional DVRs. Unlike DVR systems which have bolted on internet features along the way, dedicated cloud video solutions have been built to take advantage of the internet from day one, offering features such as remote video streaming and data back-up in a more reliable and user-friendly way. However, they often suffer from the same vulnerabilities as those found in traditional DVRs.

Inbound RTSP connections to IP cameras

Most IP cameras support incoming connections using Real-Time Streaming Protocol (RTSP). This allows video from the camera to be viewed from another machine. RTSP is very widely used; a scan of the internet shows that there are about 2.4million devices running RTSP. Approximately 1.3million of these have no authentication at all, with many allowing an attacker to freely view live video remotely.

> “RTSP is very widely used; a scan of the internet shows that there are about 2.4 million devices running RTSP. Approximately 1.3 million of these have no authentication at all, with many allowing an attacker to freely view live video remotely.”

Just as with most traditional DVRs, a large number of cloud video providers recommend port forwarding to allow access to the RTSP stream of the IP cameras from outside the firewall. As outlined in the previous section, port forwarding punches a hole right through the network's security perimeter, effectively opening the network to malicious attacks.

Poor website security

Cloudview's recent passive survey of 24 popular cloud-based video websites showed that many of them were making common security mistakes. These include:

1. Use of insecure protocols

A number of the sites did not use secure protocols to ensure that communication between the user and the site was secure. Using standard web protocol (HTTP) allows an attacker to either passively monitor, or actively tamper with, communications. Usernames and passwords can be gathered, or videos viewed.

If a website uses secure web protocol (HTTPS), the web browser highlights this by displaying a padlock in the address bar. HTTPS is the same protocol used by banks, governments and major vendors such as Apple or Microsoft. These days, it is unforgiveable for companies offering services not to use secure protocols.

© Cloudview (UK) Limited 2016

2. Poor configuration or implementation of secure protocols

While some sites did use secure protocols, they made mistakes in their configuration, massively reducing security. A significant number of sites were still found to support options that are known to be insecure. These allow an attacker to 'downgrade' the user's connection, giving the impression that the connection is secure when it is not.

"These days, it is unforgiveable for companies offering services not to use secure protocols."

HTTPS is as much about authentication as it is encryption. If companies fail to check that the server is genuine, the encryption becomes worthless. Many apps fail to check that the server is genuine, allowing an attacker to run a fake server and act as a 'middle man' in the connection, with no warning to the user.

3. No encryption or digital signatures

Encrypting the communication link is only part of the picture. Once that data has reached the cloud, how is it protected from unauthorised access, and what happens if the cloud system itself is breached?

In an ideal world, only the owner of the data (and those explicitly permitted) would be able to view it. As the data leaves the premises, it would be encrypted and only decrypted when the data is viewed by a user on their computer. Doing this with real-time, streaming video data is technically very challenging. As a result, few cloud providers offer such encryption, and most do not mention it.

Further to this, few cloud-based providers ensure the integrity of the data. How can users be sure that the video they are viewing is not from two weeks ago? How can the police be sure the video has not been tampered with? This is where digital signatures are required. A digital signature, which is difficult to copy yet easy to verify, proves that a certain device has handled a piece of data. However, few cloud-based providers use digital signatures.

4. Common website vulnerabilities

Nearly all the surveyed sites were also found to have one or more other vulnerabilities.

Cross-site request forgery

The most common vulnerability was cross-site request forgery (CSRF). This is when a user's browser is tricked into performing an action as an authenticated user. If the user was already logged into the site (even using a 'remember me' tick box), their browser would visit the link and carry out the action. The link could be sent in an email, run by a flash game or carried out in the background by JavaScript running on a web page.

Cookie security

Many sites suffered from cookie and session token security misconfigurations. If an attacker can capture a cookie containing a session token, they can masquerade as the logged-in user. It is therefore important to protect cookies; modern browsers have many features to do this. One of these features is an option called 'HttpOnly'.

The server indicates to the browser using this flag that it should not let the cookie be read by client-side code such as JavaScript. There are very few cases where setting the 'HttpOnly' flag will cause a problem; nevertheless, a large number of cloud video providers fail to set this flag.

Direct object references

Several cloud video providers were found to store video across multiple servers. Access to the videos was controlled using a long, seemingly random identifier in the URL. No username, password, or session token was required but as long as the identifier is long and random enough, this should be an adequate way of protecting content. In the case of several systems, however, mistakes were made. One system was found to use sequential identifiers, so simply incrementing the identifier would allow other videos to be viewed.

5. No controls around access to customer data

These days, users are used to accepting lengthy Terms and Conditions, End User License Agreements and Privacy Policies but few people actually read the details. On examining many cloud providers' documentation, very few of them explicitly mention what controls they have around access to customer data.

"When we are talking about sensitive data such as CCTV stored on a server as part of a paid-for service, there should be no need to share user data with a third party."

The 1998 Data Protection Act outlines a number of steps that organisations must take to preserve the confidentiality of gathered data. In the interests of all parties, companies need to ensure that they have strictly defined controls around the access to, and management of, customer data, and cloud providers should be transparent about them.

Beyond this, many cloud-based providers have clauses allowing them to share data with third parties. However, when we are talking about sensitive data such as CCTV stored on a server as part of a paid-for service, there should be no need to share user data with a third party without the explicit consent of the user.

© Cloudview (UK) Limited 2016

Conclusion

It should be clear that neither traditional DVRs nor newer cloud video systems provide the high levels of security necessary for the protection of sensitive data gathered by visual surveillance operators. Not only are such systems vulnerable to attack from external forces — compromising the security of the entire network — but the operators themselves are also in danger of failing to comply with data protection legislation. Indeed, very few operators currently reach the standards required, due to the failure of manufacturers to provide adequate access and storage controls, implement protocols or defend against malevolent intrusions.

> "Compromising the security of the entire network... "
>
> "Security cannot be bolted on. Services must be designed to be secure from the ground up."

As visual surveillance grows ever more important, companies must move away from inherent vulnerabilities in DVRs and IP cameras and embrace the technology of the cloud — provided that the cloud solution has the necessary security safeguards to mitigate the common flaws outlined on previous pages. Security cannot be bolted on. Services must be designed to be secure from the ground up; and if organisations are to protect their assets effectively, transparent security must be at the top of the agenda.

The research was commissioned by Cloudview and carried out by an independent security consultant in December 2015. Five routers, DVRs and IP cameras running the latest software were placed on the open internet. Many tests were performed, including but not limited to:

1. Passive monitoring of all traffic in and out of each device, with the aim of both working out how the device communicates, and uncovering any hidden or undesired functionality.
2. Active scanning of all ports and services using Nmap to find hidden services and insecurities.
3. Manual and automated testing of any web interfaces using Burp Suite, to find vulnerabilities and hidden functionality.
4. Decompilation of Android and iOS applications available to understand operation.
5. Obtaining firmware via downloading, intercepting firmware updates, or recovery from device.
6. Analysis of firmware using various tools to find hidden functionality, vulnerabilities, and passwords.

© Cloudview (UK) Limited 2016

How to build a ***secure*** cloud video surveillance system: Cloudview's approach

Cloudview takes a comprehensive and unique approach to security in order to protect against the numerous flaws found in both traditional DVR and many cloud video services.

No port forwarding

Cloudview does not require an inbound connection to its Visual Network Adaptor (VNA – the device which takes the images from your CCTV system and connects them to an external cloud service). All connections made are outbound, keeping the firewall intact, so there is no way for an attacker to connect directly to the device.

Invisible to attackers

As the Cloudview VNA does not accept any inbound connections, it cannot be found via an IP address, searching for Dynamic DNS addresses or scanning for specific port numbers.

Regular firmware updates

Unlike most systems that stop receiving updates a few months after shipping, the Cloudview VNA receives regular, automatic firmware updates. Because of the absence of risky inbound connections, most updates tend to be functionality upgrades rather than security fixes.

Single purpose device

The Cloudview VNA is a single-purpose device, with extremely limited scope to do anything beyond what it was designed for. In contrast to the powerful hardware and full operating system of a DVR, the Cloudview VNA does not have the necessary processing power or storage to be a useful base from which to attack the rest of the network. It only ever connects to the Cloudview platform, carrying one-way traffic securely to the cloud, and its tiny on-board storage means the risk of data exfiltration is negligible.

Use of encryption and digital signatures

Encrypting real-time, streaming video data is technically very challenging. However, this is what Cloudview does, using end-to-end encryption. It is also one of the only providers utilising digital signatures, giving companies the guarantee they need that the video has come from their device, while highlighting immediately if that video has been tampered with.

© Cloudview (UK) Limited 2016

About Cloudview

Founded in 2012, Cloudview is the world's first corporate-grade, secure, cloud-based video surveillance system. It enables authorized users to view, manage and share footage generated by CCTV from multiple locations on any smartphone, tablet or PC.

Cloudview was recently awarded 'Police Preferred Specification' status, the only CCTV product of any description to have received this accolade. The firm works in partnership with Care Protect, which has adopted Cloudview's technology across a number of care homes, and with housing associations such as Accent Group and mhs homes to protect the wellbeing of thousands of residents and staff.

Cloudview is headquartered in Hampshire, with development teams in Amman, Jordan and Northampton, England.

Contact details

Phone: +44 (0) 203 436 1100
Email: cctv@cloudview.co
Web: cloudview.co

Cloudview (UK) Limited
Pinewood, Chineham Business Park
Crockford Lane
Basingstoke
Hampshire
RG24 8AL

© Cloudview (UK) Limited 2016

All specifications subject to change. E&OE. All sales of Cloudview Services and Products are subject to the terms and conditions of use and sales of Cloudview Limited and Cloudview (UK) Limited.