ic2 DESIGN INSTALL PROTECT

12 ways to protect CCTV from cyber attack

A guide to preventing your CCTV and integrated security systems from being hacked

www.ic2cctv.com

Introduction

The internet is a double edged sword; on one hand it is a fantastic enabler of business and learning; on the other, it is the vehicle for a range of criminal activities.

From the dark web, where illicit materials may be traded, to instructions on how to pick locks and hack, the web is awash with criminal enterprise. However, the biggest internet-borne threat remains cyber crime.

This takes many guises. Much of it is geared toward fraudulent access of credit and bank accounts.
Some examples of these attacks are:

- Hacking, to steal databases containing the personal details, logins and passwords of millions of account holders
- Phishing, using emails and fake websites to trick people into revealing information that can be used to access accounts
- Malware, that uses keystroke loggers to transmit usernames and passwords back to the criminals

Other sophisticated malware attacks use ‘ransomware’ to encrypt the victims computer or server data and only release and revert it to its unencrypted form on payment in what seems to be the untraceable bitcoin digital currency system.

Defending a business against cyber attack is critical, but it’s not just about preventing fraudulent access to bank accounts and blackmail with ransomware. One of the most extraordinary hacks targeted the notorious extra-marital affairs website Ashley Madison. Stolen information from over 30 million accounts was publicly posted after the site’s owners failed to comply with the attacker’s demands for it to shut down its services.

When it comes to CCTV, the data protection act enshrines the right to privacy and Personally Identifiable Information (PII) must be handled in line with compliance regulations set out by the information Commissioner’s Office (ICO).

It’s not just about privacy and compliance with the DPA and the ICO; the converged nature of IT and integrated security systems means a hacker may be able to gain access and disable or interfere with the correct operation of security systems. This might enable a site with high value items such as artworks or bullion to be physically compromised.

In an era where there is an elevated global terror threat, integrated security is pivotal in defending major infrastructure and places where people gather. Poor system security practice could have consequences of the most serious kind.

In this guide we discuss how to defend against cyber attack to prevent CCTV and integrated security systems from being breached.

1. Consider buying from a reliable source

Choose your service providers carefully. Supply and installation services should only be commissioned from firms with engineers that are trained in the technology and which hold full certification and any other appropriate accreditation. Poor quality components and / or poor installation may create security loopholes which cyber attackers might be able to discover and exploit.

Good quality firms are likely to be accredited to the National Security Inspectorate (NSI), the British Standards Institute (BSI) and the ISO 9001 quality management system. Those that specialise in installing and supporting integrated systems are likely to be able to provide a much more comprehensive service over the lifecycle of the system.

2. Think carefully about the choice of hardware

A reputable supplier should specify good quality equipment from reliable manufacturers which are tried and tested. Generally, reputable security firms avoid budget and consumer brands and opt for professional quality equipment.

In the summer of 2016, concerns were raised that certain CCTV products sourced from a manufacturer controlled by the Chinese government and deployed across the public sector in the UK may pose a security risk. There is no concrete evidence to support this claim in the public domain, but it seeds doubts. In the autumn of 2016 weak security caused another Chinese manufacturer's products to be hi-jacked for cyber attacks.

As a rule of thumb, selecting brands with a flawless track record and over which there are no such question marks.

3. Get full training

Training is essential to getting the most out of any investment in CCTV and integrated security solution. Make sure the service provider is able to provide training and ongoing support for users as well as the installation itself.

The best service providers are able to assist with training that ensures your operators understand their obligations for meeting compliance with the regulatory code.

4. Separate the IT network from networked IP CCTV

To minimise the risk of any security breach of the IT system providing unauthorised access to CCTV surveillance, use different switches and routers to isolate the IT and the security systems.

Across larger sites, where there are multiple cameras, the bandwidth requirement of networked CCTV is substantial. On a network that mixes CCTV video streams with IT system traffic, there is likely to be significant performance issues for IT, so separation is essential.

5. Practice strong password policies

Users of the system should have individual logons and strong password practice should be implemented. The systems should force changes frequently. Consider the use of Dual Factor Authentication (2FA) systems which provide a fob that generates a one-time key (OTK) or requires an alternative secondary piece of security information to be entered by the user.

Single sign-on and password management apps both help to overcome the security problems of weak passwords and that of username and password re-use that is widely used for gaining access to multiple accounts, both personal and for business.

6. Avoid remote accessing the system from public Wi-Fi

Only use secured private connections to remotely access your CCTV and integrated security systems. Public Wi-Fi, such as that found in coffee shops, is unsecured and other users of the public Wi-Fi may be using it for criminal purposes, such as intercepting usernames and passwords to hack or commit financial fraud.

If you are using mobile devices to connect to your security system at the installation site(s), the Wi-Fi access to the security network should only be enabled using WP2A security encryption. Do not broadcast the SSID so it can be seen by Wi-Fi devices.

7. Avoid cloud-based CCTV and integrated security systems

Cloud systems for security are those that store all monitoring data offsite in the cloud - a remote datacentre - connected over the internet to the camera and other monitoring devices. There are drawbacks to these systems.

Primarily, they are only as good as the bandwidth of the internet connection over which they connect to the cloud. Several HD cameras generate a significant amount of traffic. The connection might be incapable of transmitting all the data to enable recording video streams of the required quality.

8. Automatically update software

For all the elements of a CCTV and integrated security system, and where ever it is supported by the hardware, automatic software updates should be enabled. Updates are frequently released to patch recently discovered flaws or vulnerabilities which hackers may be able to exploit.

Whether it is network infrastructure or security appliances, or cameras, Network Video Recorder (NVR) servers or PCs with video analytics software, make sure the software is up to date. If you are uncertain, check the arrangements for updating the system components with your service provider.

9. Prevent physical access to CCTV and integrated security system components

Make sure access to the physical elements of the CCTV and integrated security system is fully secured. Cameras should be positioned so that they and their power / wired network connections cannot be tampered with. NVRs and switches should be in secured areas where they cannot be switched off, such as locked server rooms.

Prevent unauthorised access to areas where video is monitored, as unauthorised access to the system may be possible through an unattended and unlocked computer or other device. If using mobile devices, configure them to delete all data after repeated failed access attempts in case they are lost or stolen.

10. Disable common access on network switches

Hackers often exploit network switch ports 80 (http) and 21 and 23 (Telnet) so make sure these and any others are disabled.

11. Think about the benefit of creating unique subnet and IP addresses

Improve security by placing individual departments on individual subnets. Preventing computers and devices on one segment from connecting directly with other segments reduces security risks.

Network administrators may choose to place all wireless clients on a single subnet, restricting the amount of the network that could be immediately attacked if it is exposed to a wireless hack

12. Consider locking down the network using MAC addressing

Each product in an IP-based security system has a unique MAC (Media Access Control) address. A suitable managed switch allows the security system to use MAC addressing to control access to the computers, cameras and network video recording devices.

Using MAC addressing, cameras can be assigned to specific ports as well as security system computers for control and monitoring. This would prevent unrecognised MAC addresses – either unauthorised internal computers or externally located hackers - gaining access.

SUMMARY

How iC2 helps you secure access to your CCTV system

iC2 is a leading mid-market security systems provider and was established in 2001. The business is owned and managed by a team with a collective experience of over 100 years in the electronic security business. iC2 holds CCTV and security accreditations with NSI and BSI.

Many of the suggestions above form part of best practice derived from ISO 27001, the internationally recognised standard for information security. iC2 installs, maintains and supports all network security installations in compliance:

- H&SE
- ICO/DPA code of practice
- IT security best practice

A prestigious client list including luxury international boutique brands, top flight sporting venues, retail developments and educational and social environments demonstrates how solutions are deployed to meet a variety of requirements.

From deterring theft of high value luxury goods, to sports fan and public safety and child protection, solutions are deployed to meet a range of legitimate purposes for which they are appropriate and fit for purpose.

REFERENCES AND FURTHER READING

In the picture: A data protection code of practice for surveillance cameras and personal information
ICO; CCTV Code of Practice; 2014
https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

CCTV's Greatest Hits: 10 top tips for movers, shakers and upgraders
ICO; CCTV Code of Practice; 2014
http://www.ic2cctv.com/white-papers/cctvs-greatest-hits-10-top-tips-movers-shakers-upgraders/

iC2 DESIGN INSTALL PROTECT

T: 020 3747 1800

E: info@ic2cctv.com

W: www.ic2cctv.com

About Us

Keeping you safe and secure at all times

iC2 provide you with innovative solutions tailored to you and your sector. We are London-based with a national team of surveyors and engineers that work closely with our clients throughout the UK and internationally.

Our unique consultative approach allows us to tailor bespoke systems to your individual requirements, ensuring that your operational requirements are met.

We appreciate the need to demonstrate the best value to you every time and as a technology-led company, you can expect our cutting-edge and ground-breaking approach to serve your needs for many years to come.

Please feel free to contact us to discuss any requirements you may have. We are happy to give you impartial advice, should you have any queries.

```
> .sf-sub-indicator
.cart-menu .cart-icon-wr
uter.transparent header#top
f-menu > li.current_page_
f-menu > li.current-menu-
ul > li > a:hover > .sf-sub
#search-btn a:hover span,
f-menu > li.current-menu-ite
.icon-salient-cart,.ascend
portant;color:#ffffff!impo
header#top nav>ul>li.butt
widget-area-toggle a i
outer.transparent
```