WATCHING BRIEF

Ola Lennartsson *examines why the cyber security of network cameras is becoming a growing concern and measures that can be taken to protect your system*

Organisations need to ensure that their CCTV network has a robust defence against potential cyber threats

The increasing availability and adoption of connected devices offers many possibilities for the security industry. Network cameras not only collect footage, but also analyse what they see and send instructions to other devices on the network to take additional actions, such as speakers or door controllers. For example, when a network camera detects a perimeter breach, it can automatically play a recorded warning to dissuade the intruder. Another camera placed at an access point can scan a license plate, and confirm whether that vehicle is permitted to access an area before activating the door opening on an access door controller, without the need of any human intervention.

Cameras are now able to recognise different types of visual data from QR codes to the number of people in a room. As well as enhancing their surveillance abilities, these new functionalities have expanded the use of cameras beyond security purposes.

Think about sustainability. It's a hot topic, especially after the latest reports on climate change, and one to which network cameras can contribute. The team of Rock Hill Schools, for example, installed cameras capable of capturing high-resolution, coloured images even in near-complete darkness, throughout its campus. This way, the campus lights didn't need to be left on during the night, reducing the school carbon footprint without sacrificing security. On a larger scale, the city of Atlanta used network cameras to monitor and regulate traffic in the city centre, reducing air pollution.

Healthcare is another sector in which network cameras have found new applications. For example, Nemours Children's Hospital in Orlando. Like all medical facilities, the hospital continuously monitors patients' vital signs. However, health cannot always be assessed by clinical data alone, due to any sudden change in a patient's condition. Since it would be impossible for medical staff to be physically present in every patient's room simultaneously, the hospital installed video cameras in each room so that paramedics can remotely monitor them. Thanks to the cameras, the staff were able to observe patients at critical moments, and immediately notify a medical team for assistance in the event of an emergency or change in their condition.

> PROACTIVE MAINTENANCE IS THE BEST WAY TO ENSURE A MORE STABLE AND SECURE SYSTEM

These are just a few examples of what innovation can bring to various sectors. However, despite all the amazing possibilities of this technology, connected devices also present risks which are dangerous to ignore. A network of cameras, if not properly secured, can offer new points of access for malicious users. Any device connected to a network can be breached, as a casino in North America realised, when in 2017 hackers entered their system via the smart fish tank in their hall, a seemingly innocuous way of keeping track of their finned friends' wellbeing.

Besides being an amusing anecdote, the fish tank hack emphasised the fact that no device is 100 percent secure, and that cyber criminals can be very creative when looking for system weaknesses.

How does an organisation realise if an attack has taken place? Unfortunately, it is not easy. The latest reports have found that most companies only realise they've been hacked as much as 191 days later, on average. Therefore, the best way to protect your network is prevention, by knowing what the potential weak points in your organisation's system are and working daily to tackle them.

Below are some of the most common ways for hackers to enter a network, providing, a solid starting point to build your defences:

PHISHING AND SOCIAL ENGINEERING

Phishing is still one of the most popular methods of hacking among cyber criminals because, despite everything, it works. We have all received some spam emails during our lives, from the most obvious scam attempts (no, that prince from a faraway land is not begging your help to transfer his money abroad) to more refined messages, that at first glance may really seem from your bank or your boss.

When carrying out a phishing operation, the hacker relies on someone clicking on a banner or a link, which can let a malware into the system or induce the victim to give up sensitive data like passwords or bank details.

This kind of attack often doesn't target a specific individual or company; the hacker just sends the same message to as many email boxes as possible and aims to trap as many users as they can. However, the so-called spear phishing email is a precisely targeted kind of scam, which also relies on research and social engineering, making it more difficult to spot.

In order to protect your devices and company, it's important to educate every member of staff to spot the warning signs of a phishing attempt. Set up a dedicated email box to evaluate suspicious messages. If a threat is discovered, staff can be easily warned and avoid falling into the trap. Also, set a policy on what can be asked for within an email; for example, forbid requests regarding log-in details or other sensitive data.

WEAK PASSWORDS

The password is one of the most important protection measures of a network, that's why you need to make sure a strong password is kept and protected, but also note to change it regularly. When a password is too simple or remains the same for a long period of time, it becomes easier for cyber criminals to hack the system.

Again, specifying password policies for your company is crucial to maintain a high level of security. It is advisable to change passwords on a regular basis, especially for accounts with admin access; set up an email reminder for you and your staff every two or three months and make sure the passwords are at least eight characters long, and contain both letters and numbers.

LOST OR STOLEN DEVICES

The first thing that you do when you realise your credit card is stolen or lost is to block it, preventing anyone from accessing your bank account. The same should be applicable in the case of a lost phone or computer, especially if it's connected to your company's network.

And that is why the BYOD trend – Bring Your Own Device, the practice of allowing employees to work and access the company data with their personal computer or smartphones – can become problematic when there are no specific company practices to regulate it. A recent survey conducted by the UK Government found that businesses that allow employees to work on their own devices, have a 49 percent higher chance of experiencing a cyber security breach. A BYOD policy may save some money on buying office devices, but at the cost of your cyber security.

SUPPLY CHAIN

Vulnerabilities are very often discovered by researchers and not by hackers. Based on the type of the vulnerability, these researchers decide their next steps. If the vulnerability is not intentional,

▶

they contact the manufacturer and give them a certain amount of time to fix the vulnerability before publishing it. However, if it is a critical vulnerability with intentional character, like a backdoor, they instantly go public to raise the awareness.

It is the duty of the manufacturers to design their devices without backdoors and hard coded passwords, as well as to supply the right tools to make cyber management for many devices both simple and affordable. They should then educate users and suppliers about the risks and how to avoid them, both internally and externally.

Finally, for a distributor, the topic of cyber security is very simple. They are just handling the logistics and do not need to touch the product itself. However, this does not mean they don't bear any responsibilities. Transparency is key: they need to let their customers know what they are buying. Without this transparency, it is typically the cost which influences the customer's decision, when purchasing a device or solution.

NOT KEEPING TECH UPDATED

Proactive maintenance is the best way to ensure a more stable and secure system in today's ecosystem of connected devices. Responsible manufacturers understand this and regularly release firmware updates to address vulnerabilities, while also fixing any other issues that may affect performance.

When you don't keep your system updated – by running older, not updated versions of software – the devices of your network are more vulnerable. This is because unpatched or not updated technology is more likely to contain weaknesses already known to cyber criminals, which can be exploited to access a network. Therefore, it is crucial to install system updates as soon as they are available.

Ultimately, who is responsible for cyber security? The simple answer is that everyone is. From the software designer, to the manufacturer, to the end user. It's a shared responsibility, much like environment preservation or recycling.

The creation and usage of connected devices are linked by a chain of actions and people. Therefore, it's more crucial now than ever that everyone dealing with this technology is warned, educated and prepared to avoid a system breach.

IF NOT PROPERLY SECURED A NETWORK CAN OFFER NEW POINTS OF ACCESS FOR MALICIOUS USERS

That's especially important in the case of the surveillance industry. As consumers start to become more concerned about their privacy and trusting companies, those who can't provide security are likely to face difficulties.

We earn the trust of our customers and partners when we do our best to protect them. Of course, employee training programs are costly, but so is eliminating legacy systems or hiring a cyber security specialist. The best investment you can do for the future is one you won't ever regret ●

Ola Lennartsson is product manager for enterprise systems, specifically focusing on cyber security, services and tools for the enterprise market. He joined Axis in 2014 bringing deep experience from a variety of product management roles.

Businesses that allow staff to work on their own devices have a 49 percent higher chance of a cyber security breach