Protecting IP video data

While not actually a UK law, the US NDAA has had some mainstream media coverage on these shores, which has raised concerns about data security in some applications

The John S. McCain National Defense Authorization Act for Fiscal Year 2019, commonly referred to as the NDAA, concerns the purchase of technology from specified vendors by the US federal government and some perceived security issues around its use. Whether a valid concern or not, securing non-compliant cameras here in the UK has also become a hot topic over the last few years despite the NDAA legislation not actually being in place over here. Some organisations, in particular US-linked businesses based in the UK, need to be aware of the Act and its stipulations and ensure that systems meet the requirements involved. UK-only companies, on the other hand are not bound by any law that restricts the use of the equipment, yet some are looking at the issue and what measures could be put into place.

One such solution is the Vemotion Video Firewall, designed to help protect high-security applications, and Local Government and Law Enforcement agencies that use non-NDAA compliant surveillance cameras and have any concerns regarding the kit they already have.

To find out more about the system, PSI spoke with Steve Haworth, Vemotion's CEO, who explained the background to the technology and why going to the expensive lengths of replacing existing cameras in an application is not necessary to secure the data on the network from any potential risk

Did you specifically develop the firewall with the NDAA in mind, or is a function of an existing product?

I'd say it was a redevelopment of an existing system. Our video streaming products already isolate cameras from networks effectively, but what we've done with this product is basically take all of the elements of our existing systems and shrunk them down to a single box solution at a price point that makes sense. We are very much aware that putting a unit next to every camera already installed is more viable than buying a whole new video streaming solution. Essentially, in terms of functionality the new firewall is a stripped-down version of an existing system but packaged at a price point that makes sense to installers and their customers. →

Steve Haworth, Vemotion CEO

"In essence, there is a lot of confusion around at the moment, which I think comes from people not knowing the full details about the real situation, rather than the way it has been covered in some media outlets"

(continued from page 19)

"Concerns will always exist, but they can be dealt with as long as we can keep up with technological developments"

What's involved with installing the firewall?

It's a piece of hardware that is fitted next to the camera in the existing application. The unit is a small box that connects the camera to the firewall and then the firewall talks directly to the VMS. In all intents and purposes, by using the firewall you are setting up a secondary network, taking the camera off the original network, meaning that the camera never has access to speak outside the network - it only links to the firewall and then the VMS. This adds security and control to the data and, in reality, using the term firewall to describe the product doesn't do it justice, because it is capable of doing a lot more than just being a firewall. What we're doing is enabling the VMS to still do pan, tilt, zoom functions and control the camera, but technically the VMS is speaking to the firewall which, in turn, is speaking to the camera. For the installer, fitting the unit is easy and there is just a one-off charge for the kit with a small annual maintenance fee.

In terms of the camera, does the system work on any make or model?

Yes it does, but for all the control and features ONVIF is a requirement, however most cameras can at least stream an image with the firewall. Of course, if you are working on an application for local government or police, you'll likely be using ONVIF cameras anyway.

As we don't have NDAA in the UK, which applications is the technology aimed at?

In development, we looked at the CCTV market and, yes, while the NDAA itself is not enforced in the UK, we thought about what would happen if there was a change in government or in legislation and then what installers and their customers would do if they had a big installed base of cameras and they needed to secure the network. We realised that by isolating the camera off the network and using a secure video firewall was the way forward. We're happy to leave the politics of the issue to governments to sort out, but from a technically secure point of view, we needed to find a solution that stopped anyone from potentially getting at the data moving from the camera to the VMS. In most cases, this is seen as a concern for the police and local government etc, but it also includes the military and critical national infrastructure installations that have an extra focus on the security element of their data.

Where do you see the concern about NDAA coming from; the installer or the end user?

It's coming from both, but I would say that it is being driven by the customer, wondering whether they are secure in carrying on using the camera technology they have in place. In essence, there is a lot of confusion around at the moment, which I think comes from people not knowing the full details about the real situation, rather than the way it has been covered in some media outlets. In general, for the police and councils that deal with crimes etc, having a camera off the network makes perfect sense for them. And in terms of budgets and, increasingly these days, sustainability, people can't just rip out and replace their existing camera investments, some of which could have been only recently installed. The customers that are seemingly most concerned about the issue have cameras that have potentially got a lot of "life" left in them, so they simply don't have the budget to pay for another installation so soon after the initial work was carried out.

Given that cameras are seen as data gathering devices today, will video data security concerns only grow?

Concerns will always exist, but they can be dealt with as long as we can keep up with technological developments. As soon as the world went over to IP, the rate of innovation around networks went up too, on the side of good and bad intentions. There are ways to effectively manage these data security issues and if you think about other sectors, such as online banking, everyday data problems are being managed as the world becomes more network reliant and new systems are launched. Video data security will need constant attention in the future, particularly as more capabilities go into networked devices, making them a more lucrative target, but it doesn't mean they shouldn't be used, it just means they will need up to date protection from any new threats going forward.