WHITE PAPER:

Top 6 Measures to Reduce Video Surveillance Cybersecurity Risks

razberi technologies

In late 2016, a massive distributed denial of service (DDoS) attack caused outages of major websites such as Amazon and Twitter. Hackers hijacked an estimated 100,000 devices, including network security cameras, into a "botnet" for the attack. The devices were infected with the "Mirai" virus, which enters a camera by logging in using one of 61 default or common weak passwords.[1] Once in place, the virus can be asked to flood any site on the web while still operating as a normal camera.

These devices were left "open" on the Internet, but even cameras on private networks are vulnerable to attack. The disruption of these sites for the better part of a day produced an unimaginable loss to the economy and wide sweeping impact on consumers.

In early 2015, a Chinese Internet Security Center was hacked using a similar technique leveraging a virus in their security cameras.[2] The cameras had been programmed to scan the building network looking for vulnerable resources.

These are just a couple of high profile attacks that have brought attention to the potential security impact of IP networked connected devices. In the physical security industry, we are pretty good at anticipating new physical security threats and adding another layer of security to protect ourselves. It is curious therefore, that we have been so slow to react to the clear and present threat of cybersecurity attacks. We all know that IP networks are a powerful platform for hosting our surveillance systems. Yet we don't spend much time thinking about the danger of our own network in the wrong hands.

Why Should You Care?

The security of the security of every organization needs attention immediately. This is not hype or scare tactics. The threat is real and it needs to be addressed. In a recent survey of more than 100 physical security professionals, one of the top concerns is lack of multi-departmental cooperation to address cybersecurity threats.[3] Physical security leaders and IT leaders need to work together. For the reasons covered in this paper, your IT staff will likely welcome an intelligent surveillance appliance strategy.

Physical security leaders and IT leaders need to work together.

1. http://www.csoonline.com/article/3126924/security/here-are-the-61-passwords-that-powered-the-mirai-iot-botnet.html
2. https://translate.google.com/translate?sl=zh-CN&tl=en&js=y&prev=_t&hl=en&ie=UTF-8&u=http%3A%2F%2Fwww1.hikvision.com%2Fcn%2Fnews_detail_63_i1273.html&edit-text=&act=url
3. Surveillance Market Intelligence Survey of more than 100 professionals www.razberi.net/survey

"But the Cameras Still Work"

Because surveillance cameras often still operate during cyber attack, and continue to capture video, your first reaction may be "why should I care?" In fact, there are three serious scenarios to consider.

1. If the camera can be asked to bombard another website with traffic, it could also be asked to take down the company's manufacturing or point of sale system. Got your attention now?
2. If someone can program the camera to send traffic, that person can program it to do other things (for example loop the last 15 seconds of video or shut it off entirely).
3. If the cameras are participating in an attack on other websites, and your network provider detects the excess traffic heading to one site, it may shut down Internet access for your organization until the issue is investigated. This is not good if your organization or company is dependent on making a living off of the Internet; and these days – who isn't?

Having a Good Firewall May Not Help

If you think this doesn't apply to you because your cameras are safe behind a firewall, think again. The 2015 "Inside Job" report from Meritalk surveyed 150 Federal Government IT managers. Nearly half of them (45%) reported an insider cybersecurity incident in the previous 12 months and 29% of those resulted in data loss.[4] The largest threat of hacking may well come from your own employees.

Sometimes the "insider treats" come from outsiders. The infamous Target® data breach of 2013 occurred because an outside contractor legitimately had a login to a vendor portal used to submit invoices.[5] The contractor had his user name and password stolen in an email hack. The hackers used it to gain access to the Target corporate network and then the point of sale system. This resulted in 70 million credit cards stolen and a $300M dollar loss.[6] Had they infected the cameras, Target could have found themselves with a second set of losses.

What Hasn't Happened (Yet)

What has become obvious in the last year is that simple devices such as security cameras must be installed and administered with cybersecurity in mind. If not, they can become huge risks to the company they are supposed to protect.

So far, the camera attacks have been focused on disrupting the business of those other than the camera owner. With code floating around the Internet that breaks into poorly protected cameras, how long will it be before hackers modify that code to attack the camera's owner?

Top 6 Measures to Take Now

Fortunately, while the risks are real, there are simple things that can substantially reduce cyber attack exposure. Here are the top measures to take to avoid cyber incidents:

1. CAMERA PASSWORDS MATTER

The number one item on the list is not to ignore camera passwords. Many installed cameras are still using the default passwords from the manufacturer. Many others have incredibly weak

What has become obvious in the last year is that simple devices such as security cameras must be installed and administered with cybersecurity in mind. If not, they can become huge risks to the organization they are supposed to protect.

4. https://www.meritalk.com/study/inside-job/
5. https://krebsonsecurity.com/2015/09/inside-target-corp-days-after-2013-breach/
6. http://www.lavasoft.com/mylavasoft/company/blog/cost-of-target%E2%80%99s-holiday-season-data-breach-300-million

passwords that are easy to guess. Either way, it can be a huge door for a hacker to walk through. Hackers write programs that try a list of default and common weak passwords. They can try hundreds of passwords very quickly hoping to stumble on one that works. In fact, the Mirai virus works exactly that way, using a list of 61 passwords like "admin" or "54321." The fact that this technique was able to infect over 400,000 devices on the Internet speaks to how many people ignore the importance of passwords.

2. ISOLATE YOUR CAMERAS

If the bad guys can't talk to your cameras, they can't attack them either. Don't make the mistake of putting them on the corporate network with all of the other PCs and Workstations. Isolate them with a Virtual LAN (VLAN). The only thing that should be able to talk to them is the Video Management System (VMS).

3. LOCK DOWN THE NETWORK

By their nature, cameras are many times located outside of the secure space, and often outside of the building. This represents a security risk, because unplugging any camera and replacing it with a laptop allows access to any camera on your network. The solution is to make sure the network is configured so that the only devices allowed to communicate over those ports are the cameras you installed. Each camera has a unique identifier called a MAC address. A network can be configured to only allow a certain MAC address on each port (a feature called MAC Binding). With this in place, all communications from other devices gets thrown away and the hacker gets a dead connection.

4. TWO OPERATORS = LESS RISK

IT departments discovered a long time ago that computers should use at least two logins: a user with a minimal amount of privileges and an administration login with full privileges. This separation of users minimizes the chances of a frequently used login falling into the wrong hands. Cameras should be set up the same way: one login used by the VMS that allows for streaming video only, and an admin login that is only used on rare occasions, such as needing to update firmware.

5. DON'T IGNORE UNUSUAL EVENTS

When someone is hacking your cameras, very often there are footprints in the sand. The camera will, of course, go offline if it gets unplugged so the hacker can plug in his laptop. That said, the hacker may try to plug the camera back in, so even a short outage should be regarded with suspicion. If a new set of firmware is uploaded, the camera will reboot. Viruses often place a load on the camera and reduce performance.

You might get lucky and notice one of these during your normal use of the system, but good security takes more than luck. The best practice is to set up the system to monitor for events like these with immediate notification.

6. PURCHASE CAMERAS FROM A COMPANY WITH A REPUTATION FOR SECURITY

There has been a considerable amount of concern over the security of certain brands of cameras. The concern has reached a point where some VMS providers are dropping full support for those manufacturers.[7] Most certainly, checking the "cyber reputation" of any system component vendor should be on your checklist prior to a major purchase. Look for vendors that have a public reputation for attention to proper cyber aware design. They should also have a rapid response to any vulnerabilities that may be found as well as a general level of trust.

If you already have a significant investment in cameras from a less than trustworthy vendor, note that following the preceding five recommendations will significantly lower risk.

Automated Solutions to the Rescue

Unfortunately, there is a problem with these recommendations: they require dedication and a level of effort to be effective. Security leaders already have a lot to deal with on limited time and budgets. As a result, security directors often ignore the cybersecurity status of their cameras, and

7. https://ipvm.com/reports/genetec-hikvision

installers fail to raise the issue with their customers. It doesn't take a CCNA certification to be proactive on cybersecurity protection, but it does require the right solutions and attention to the problem.

Security professionals need the administration of these best practices to be scalable and automated. In addition, there are opportunities to architect the video surveillance network in a way that lowers the burden of this effort and increases the security and manageability of IP based cameras.

Razberi Technologies is at the forefront of this challenge by offering Razberi ServerSwitchIQ™ intelligent surveillance appliances. The appliances combine a server, managed switch, PoE, easy to use software and VMS integration into a powerful surveillance solution. The software includes Razberi CameraDefense™ for automated camera hardening and Razberi VyneWatch™ to provide cyber threat monitoring.

There are three pillars of the solution that provide layers of proactive security:

- Automated Camera Hardening
- Secure Appliance Architecture
- Cyber Threat Monitoring

The best practice measures outlined in this paper are addressed with automated solutions and artificial intelligence to protect IP-based surveillance systems. Let's walk them through one by one:

AUTOMATED CAMERA HARDENING

Razberi ServerSwitchIQ intelligent appliances support Razberi CameraDefense™ which automates camera hardening.
It serves to:

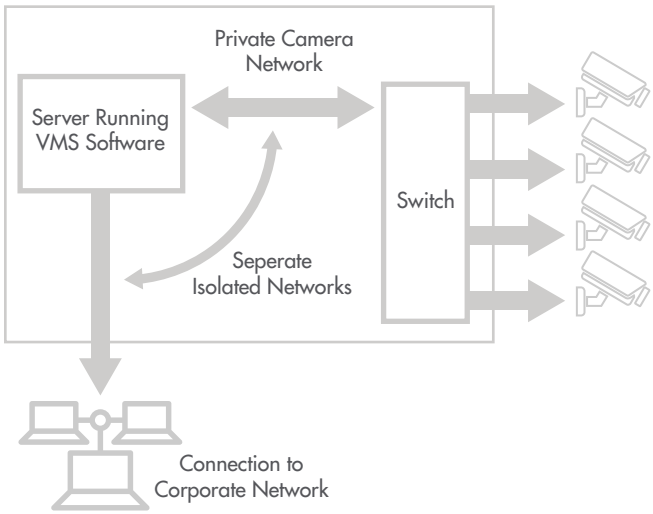
- Block unauthorized IoT devices: It binds cameras and other IoT security devices to the network and prevents unauthorized devices from using Ethernet connections.
- Secure access to cameras: Restricts camera access to whitelisted IP addresses, blocks camera traffic to the public Internet, flags weak passwords.
- Protect from cyber attack: Denies un-needed and potentially dangerous camera services with a next generation firewall.

SECURE APPLIANCE ARCHITECTURE

A major differentiator of using an appliance architecture for surveillance as opposed to a centralized, general-purpose server is the ability to keep cameras isolated from the network. There are three key aspects of the architecture:

- Isolated camera network: Separates the camera network from the business network with independent network interfaces and a configurable VLAN.
- Encryption-ready hardware: Supports video encryption and trusted system boots with an embedded Trusted Platform Module (TPM).
- Integrated virus and malware protection: Protects the video management system by predicting known and unknown attacks to proactively prevent malware execution. Razberi appliances are powered by Cylance PROTECT, using artificial intelligence (AI) to predict, prevent and protect the appliance more effectively than traditional signature-based anti-virus products.

Razberi ServerSwitchIQ in a VLAN Architecture



CYBER THREAT MONITORING

The final pillar of effective cybersecurity protection is the ability to monitor what's going on in the system including appliances and down to cameras. Increasingly, cloud-based tools are being used to automate monitoring and IT services. Razberi's intelligent appliances include a cloud-based health monitoring feature called VyneWatch™ and the ability to integrate with leading VMS solutions for monitoring and threat notifications. It provides:

- Real-time security alerts: Generates SMS text, email and real-time security alerts for incident response.
- Flexible alert management: Manages security alerts with Razberi VyneWatch™, Milestone XProtect® and other certified VMS products.
- Dynamic threat protection: Evolves with new threats to stay ahead of hackers through machine learning and artificial intelligence (AI) versus the need for an internet connection for regular signature-based updates.

ACTING TOMORROW IS TOO LATE

Security is more complex than ever and the convergence of physical and IT security is upon us. There are pragmatic efforts that organizations should take right away. Razberi solutions make the job easier and cost effective. Razberi intelligent appliances with CameraDefense and VyneWatch lower the burden of megapixel video on the network, automate camera hardening, provide a secure appliance architecture and offers proactive cyber threat monitoring. It means you get back to your most important day job – keeping the organization physically secure without opening it to new cyber attack threats.

Contact Razberi Technologies today to request a demonstration and discover what the intelligent surveillance appliance can do for you at: www.razberi.net

Razberi Technologies offers a reliable, secure, and network-friendly video surveillance infrastructure that records the highest quality video while reducing capital, bandwidth, and space costs. Razberi ServerSwitchIQ™appliances uniquely combine a firewall, PoE switch, server, storage, and intelligence. Deployed in a scalable architecture near the network's edge, the platform enables organizations to decrease network utilization by up to 95 percent and protect cameras from cyber attacks. Embedded Razberi CameraDefense™ software automates cybersecurity protections with camera hardening and cyber threat monitoring. Built-in Razberi VyneWatch™ health monitoring software alerts security professionals to issues 24×7. Razberi appliances are compatible with top video management systems (VMS) and any network camera. For more information, visit razberi.net.

razberi™ technologies

Americas: 469-828-3380
UK/EMEA: 0203 773 3689
salesinfo@razberi.net

wpcs20170503