SEC

SECURITY EXECUTIVE COUNCIL

A research and advisory firm

Network Protection for Security Systems

Ray Bernard, PSP, CHS-III

Originally Published in SecurityInfoWatch.com

April 2010

Network Protection for Security Systems

Networked security systems have a variety of vulnerabilities, and even standalone systems are not vulnerability-free. Security system networks can also have unique vulnerabilities that do not occur with business networks. The questions below were posed during a tech lab at ISC West around best practices for protecting IP-based security systems (www.BPforIP.com), where you can download two white papers relating to this topic. In this issue's column, I'm posing questions for you, the reader, to answer.

Q: The corporate network is being attacked from an internal location. Your security systems are connected to it. How do you respond?

One security practitioner I know received such a notification; however, this would not happen for most companies, given the typical project-based level of collaboration between Physical/Corporate security departments and the IT department. Security systems could be affected without the Security department knowing what was going on. What condition would warrant Security being notified of a probable network attack? What response procedures would you follow? Most security technologists have not thought through these kinds of scenarios.

Q: A disgruntled employee has just taken out a lobby security camera with a taser. This also took out the network switch the camera was connected to. What should you do next to protect your security systems in this kind of scenario?

Starting a few years ago, as part of security risk assessments, I and a few other security consultants began using Internet searches to help determine the likelihood of attacks that formerly would only be known about by people with special training. During one security assessment, a facilities engineer stated that he thinks every so often about the easy access to the transformers on the edge of the property, because it would be easy to take them out using a particular technique (using a $3.00 item purchased at a hardware store). He said, "I don't think it's a serious concern because only trained engineers know about this vulnerability."

An Internet search instantly brought up a link to a Web page where the girlfriend of an engineer, who is a member of an activist group, described the attack in detail, including the $3.00 item needed. She

wrote, "Use this approach to selectively take out power to specific facilities, rather than taking down an entire area, which might include hospitals or other healthcare facilities. You want to target businesses where loss of life is not the likely result."

Learning about the camera taser attack, I did an Internet search on that topic, and found a YouTube video showing how to make a taser from the type of disposable photo camera available at most drugstores. So what I thought was an attack that required the purchase of special equipment, turned out to be not-so-expensive.

Rodney Thayer, CTO of Secorix (www.Secorix.com), performed lab tests using a Graybar lighting arrestor connected between the camera and the network switch. Directly tasering the camera did not take out the network switch when the lighting arrestor was installed.

Most integrators that I know use fiber modems to connect to outdoor cameras, specifically due to lightning vulnerability. Additionally, this keeps the network connection inside the building. However, I do know of two Bay Area high-tech companies that have installed network cameras outside their buildings, with a network connection going right to the camera. This is like opening an outside door to the server room, as far as the network switch is concerned.

Another important point about lightning vulnerability is that the power behind a lightning strike is considerable. A lightning strike to a network camera connected by copper cable may very well take out a series of network switches, not just the first connected switch. And there is also the life-safety risk of impacting a technician working on any of the connected equipment.

Q: How would your IT department respond to a network attack that is coming from inside a facility, behind the corporate network's external firewall? How would they detect, assess and respond to such an attack? Do you have equivalent technical and procedural measures in place, either through security department capabilities or by a service agreement with IT?

It is worth exploring the insider network attack scenario with IT, as it can apply to security networks. How quickly can you tell when a network camera is disconnected from the network? Will it go undetected until the video loss is noticed, or will someone receive a video loss alarm? Are the cameras monitored the same way that critical IT equipment is monitored, so that the loss of the network

connection is immediately reported? What about an IP card reader that is disconnected? Will that only generate an access control system alert to a security officer, or will network monitoring also provide notification to someone who can address the problem?

If you are still thinking of your security systems network as an installed network, then it is time to start thinking of it and treating it as a managed network. Hopefully you have followed the IT department's standards and guidelines, so that the security systems network can be managed as well as the corporate business network can be managed.

If you have convergence experience you want to share, e-mail your comments to me at **ConvergenceQA@go-rbcs.com** or call me at 949-831-6788. If you have a question you would like answered, I'd like to see it. We don't need to reveal your name or company name in the column. I look forward to hearing from you!

*Ray Bernard, PSP, CHS-III is the principal consultant for Ray Bernard Consulting Services (RBCS), a firm that provides security consulting services for public and private facilities. Mr. Bernard has also provided pivotal strategic and technical advice in the security and building automation industries for more than 22 years. He is founder and publisher of The Security Minute 60-second newsletter (**www.TheSecurityMinute.com**). For more information about Ray Bernard and RBCS go to **www.go-rbcs.com** or call 949-831-6788. Mr. Bernard is also a member of the Subject Matter Expert Faculty of the Security Executive Council (**www.SecurityExecutiveCouncil.com**).*

About the Security Executive Council

We are a research and advisory firm for security leaders. We have a collective of close to 100 security subject matter experts that have been successful security executives or are recognized industry experts in their field. The resources and tools we develop are constantly evolving to provide maximum value. Some engage with us by way of multi-year "retained" services agreements (Tier 1 Stakeholders). Tier 1 Stakeholders are those that want support on an ongoing basis but also want to have an active role in identifying solutions for the industry. Others come to us seeking a specific solution to a contained issue. In all the ways people engage with the SEC the bottom line goal is to help define and communicate the value of the Security organization.

Contact us at: contact@secleader.com
Learn more about the SEC here: https://www.securityexecutivecouncil.com