Understanding Cyber Threats to Electronic Security Systems

For many years the Security Industry has been designing and installing their systems inside their own IT networks in order to communicate to their peripherals via network architecture. These networks were then and still are now composed of complex data control and power-cable infrastructure. There were not many outside threats, other than threats coming from land-line telephone systems… since we were still using dial up modems!

With the advent of Network Communications and with more data demands from our Electronic Security Systems (ESS), there came a push toward connecting ESS systems to existing Network systems, typically controlled by an IT department. Most ESS Systems are not designed with Network Security in mind, as we trust that the Network Security in any given network is accomplishing its purpose of protecting the network infrastructure

The recent, continuing tsunami of cyber-attacks to almost all systems (from satellite communication, SCADA systems, CCTV, and wireless communication, among others) is rushing integrators and manufacturers to come up with solutions. And that is becoming a major task, since attacks can come from many angles within ***any*** type of system. Many new start-up companies are also coming into play, and many of the existing Network Security manufacturers are also finding that their systems are not as secure as they once thought they were. Security Networks are not the only problem… we also know for a fact that USB devices can be infected with malware, as are other microchips being used in many computers. All of this adds to the massive confusion of the Cyber Security industry and multiplies the threats and vulnerabilities of a system.

Trust of IT Networks and Software Security is no longer a reality since we are witnessing exploitations coming from everywhere, from databases to USB ports, amongst others. Patches from the diversity of operating systems like Linux, to Windows OS, to Android OS, are not properly managed; firmware updates are now another concern.

Big Data is also another huge concern, since our ESS systems must collect larger data from video and audio sources. This creates a big problem for the integrator as well as the installer, since malware attacks can easily wipe out important evidence that may have been captured via recording devices, such as a DVR or NVR. Some installers of ESS Systems are also not changing default passwords, or not shutting the communication ports of ESS peripherals. Some of those devices are also poorly designed, with weak access control to their peripherals. Throw in the use of simple username/password and your faced with many possible holes into a network!

We now can understand that our Electronic Security Systems are similar to IT Information Systems (with the composition of Hardware, Software and Data); however, one additional component to ESS Systems is that of the ***Control System.*** We use several methods of wireless communication devices to connect access control systems, cameras, et cetera, and we have learned that Wi-Fi or other wireless

technologies are not trustworthy enough to use them. And by encrypting that communication, it makes an impact on the video communication speed.

Black Hat conferences are touching upon these issues in a high level manner and also are providing live demonstrations of how vulnerable some peripherals of ESS Systems actually are. The ESS industry should really pay close attention to what these people are saying… to learn from them in a proactive manner instead of just sticking our heads in the sand. Many new incumbent technologies are coming up as part of integration with ESS Systems, one for instance is the use of cellular technology using Smart phones as a way to access a facility. We should make sure that these technologies are well protected! At a recent Black Hat conference, experts in the field of cellular technologies have been able to demonstrate how simple it is to take over a cell phone by intercepting information transfers through their wireless communication devices.

The vulnerabilities that affect our system are the same as IT information systems, from wireless communications, to operation systems, to the firmware of a device and/ or an infected USB device. While an IT Information manager is mainly protecting databases, which may have bank account or financial information, et cetera, ESS integrators and manufacturers are concerned with protecting from an attack where access is gained to our control devices. This could be a major problem for a facility or an infrastructure that we are protecting!

To summarize and fully understand the problem, we must first conceive that Security begins with Security Access Control and Identification systems, and this applies to Physical, Logical ***and Cyber Security***. Intrusion Detection is also as important to protect the perimeter of your facility as it is to the perimeter of your ***virtual*** walls. Thus, we need to protect the internal areas of the facility, just as we need to be mindful of protection of data-centers and network communication hubs. We need to understand how to protect access to that database or those documents that are residing in our datacenters or on our servers.

Jorge G. Lozano
CEO/President
Condortech Services, Inc.
6621 A Electronic Drive
Springfield, VA 22151
www.condortech.com
P: 703-916-9200
Twitter