CYBER THREATS TO PHYSICAL SECURITY SYSTEMS

We all know that critical infrastructure can be vulnerable to cyber-attacks. Firewalls protect unauthorized access to and from a private computer network. These Firewalls may need the support of other IT security appliances or devices to properly protect the complex networked information systems so servers and computers are not infected by Malware, Viruses or any other unknown new threats, which have become increasingly sophisticated. These threats can penetrate and attack various edge devices, such as workstations and servers along with mobile devices.

The reality is that most Firewalls are not designed to protect ESS Systems or SCADA Systems, from sophisticated cyber-attacks; putting operating capability essentials at risk. We all are aware of the sophisticated attacks of the stuxnet worm which was designed to attack industrial Programmable Logical Controllers (PLC); this ruined almost one-fifth of Iran's nuclear centrifuges. Each year, damage to critical infrastructure from network incidents and cyber-attacks is measured by billions of dollars.

We also learned recently that some mobile bellular technology is succeptable to such attacks and that includes a majority of edge devices that are connected to networks such as home alarm and even medical devices.

Traditionally, ESS systems were not designed to be networked over the IT infrastructure, these ESS Systems have their own stand-alone networks As a result of 9/11, the impact to get the most data from ESS systems, as well as to be more efficient in investigating crime and research of potential vulnerabilities; more and more ESS Systems have been integrated into the IT network infrastructures.

Many hazards result from institutions' demand of more video-data and audio coming from the ESS systems, which results in growing numbers of physical security peripherals (PLC, RTU, Controllers, Microcontrollers, etc.) being connected to the IT networks infrastructure of the facility. These networks are not fully capable to protect these sub-systems of these network's technical staff clearly understand these ESS systems in depth and detail. We are witnessing and increasing number of attacks, on physical security systems that are connected to these networks and the need for a comprehensive solution is now a reality.

Most ESS peripherals use a diversity of devices and sub-peripherals similar to SCADA systems, with proprietary embedded operating systems (OS). These peripherals allow the automation of electromechanical processes such as those used to control machinery on factory assembly lines, amusement rides, open or close doors and other ESS operations.

These peripherals are known in the security industry by specific names, depending of the manufacturer of the ESS; and most of them use the same technical foundation to operate. A minimum number of these peripherals meet NIST standard like FIPS 140-2, and most cannot protect properly from specialized cyber-attacks; and their communication ports to the networks have vulnerabilities. The use of these unsecured networks exposes ESS to cyber-attacks:

- Video streams from cameras can be replaced or manipulated.

- Control can be hacked to open gates and doors.
- Perimeter security sensors and controllers can be disabled
- WIFI and other wireless communications can be disabled

In order to solve this challenge that goes beyond the traditional use of firewall security, these ESS systems will need a better tailored network protection solution for assorted zones of devices and peripherals. ESS systems have to be designed with a clear understanding of these new environments and threats, with advanced IT security technical skills and understanding of the electronic security industry in mind, while being implemented without system downtime.

The use of cutting edge hardware, along with network intelligence and policy-enforcement software engines, offers an effective tool for securing and hardening sites and installations.

The ESS Cyber Solution acts as a powerful security policy enforcement tool, allowing the user to:

- Detect and identify every element and endpoint in network
- Alert or block any attempt to connect an unauthorized device.
- Inspect all traffic at port level to make sure that only safe and identified traffic is allowed.
- Detect Layer2 and Layer3 cyber-attacks: CAM overflow, ARP spoofing or poisoning, IP address spoofing, video hijacking, Protocol manipulation, DoS, etc.
- Report and take automatic action to restore continuous and safe operation of the network.
- HW protection, making the switch policy-enforcement tamper-proof.

In summary, the ESS systems and their infrastructure are at risk of cyber attacks. The existing network security protocols in place do not meet the needs to protect these systems.