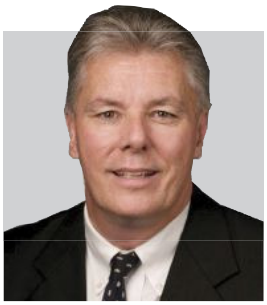
IT Intelligence

TAKING STOCK OF RETAIL'S EXTRA SECURITY LAYERS

by Bob Stockwell



Bob Stockwell is Chief Technology Officer for STANLEY Security. From 1997-2012, he was Niscayah's Director of Systems Operations.

bob.stockwell@sbdinc.com

Security system devices in the current retail environment are designed to provide physical protection, but what if those systems become compromised? What type of protection is available? Can simple security systems — including alarm, access control and CCTV systems — be turned into vulnerable access points to create customer disruption?

By validating and protecting security hardware, retailers can create another layer of protection to keep intellectual property safe in the event that the security system is compromised. Most, if not all, of today's systems are network-enabled and can be vulnerable if not properly tested and protected.

Following are some tips and key things to remember when protecting security systems in a retail environment.

DIVIDE NETWORKS AND CONQUER TRAFFIC

One of the first and most effective steps that can be taken to protect all facets of security hardware is to separate key system platforms. The challenge lies in finding a cost-effective solution to achieve this, especially if both systems are already on the same network and there may not be enough capital to build totally separate networks. If not already in place, consider replacing older data switches with newer devices that can be remotely managed. This allows the IT department to create VLANs (virtual local area networks) at each location without building a totally separate network. This virtually separates existing data systems so that they don't comingle with the POS (point-of-service) or customer data, and also separates security hardware devices. This protects the space from a potential attack launched within the internal network if the security systems were to be compromised or accessed as a delivery path for disruptive malware.

Firewalls can also serve as reliable means of protection when configured and managed properly, acting as the first line of defense against the outside world. Understanding what the space's internal systems do and how they communicate will allow storeowners and managers to better define firewall rules and alerts. It can take some time to isolate the type of data and the ports needed to communicate, but every open port is one more point of access that someone might attack and exploit to gain unauthorized entry into or damage the security systems. Therefore, only allow the minimum communication needed for systems to function.

Know what data traffic is expected on the internal network and create alerts for abnormalities. Most firewalls have a feature called "stateful inspection." This allows users to define what type of traffic is allowed and how it can communicate. For example, many systems allow E-mail traffic, which communicates on a standard port number. If the firewall system were to recognize traffic on the E-mail port that was not E-mail (e.g., Telnet), it would block that data and send an alert to the system administrator.

Only allow system access to those who require it, and only at the necessary level. Because of how detailed many systems have become, storeowners are tempted to throw up their hands in frustration and grant all personnel full access. Instead, take the time with clients to determine exactly what an individual needs to carry out his or her role, and define that system access. This eliminates the risk of less knowledgeable or untrained personnel from causing damage to crucial systems.

BE WARY OF PASSWORDS, VISITORS

Also advise retailers to change default passwords, and disable or change the default user accounts on systems and devices. Every system is equipped with an administrator account, and best practices suggest that users should change this account name and definitely change the password. Also, don't forget to look at end devices, such as IP cameras, which have default usernames and passwords that should be changed as well.

Only allow system access to those who require it, and only at the necessary level. Because of how detailed systems have become, storeowners are tempted to throw up their hands in frustration and grant all personnel full access.

Make sure your retail clients' employees are educated on how to work with and monitor visiting vendors and what to expect. For example, grocery store employees must know that a soda distributor should not be in the data or phone closet. Many of today's attacks come from inside, and can be as simple as plugging in a USB drive for just a few seconds. While it can be tricky to monitor all activity of an outside vendor at a retail location, creating and enforcing a vendor monitoring policy establishes an environment in which it's more difficult to compromise the security systems in place. SSI