VIDEO SURVEILLANCE

MAINTAINING YOUR CYBERSECURITY

By: Chris Garner

Today's security networks have evolved from where they were 20 years ago. With these changes, we have seen many amazing advances in the technology and the connectivity between the systems which comprise today's complex security systems. Through these advancements has also come concerns on how we secure these systems and the data within them. As we look through the headlines, it seems a new data breach or network vulnerability is exposed daily, and this is why securing our system should be a top priority.

In cybersecurity, many refer to the three pillars for security, which are confidentiality, integrity, and availability. But what do these pillars represent, and how do we address these? Confidentiality is often considered the primary goal of security. To maintain confidentiality, the system and data should only be accessible to authorized users. To address the concern or integrity, the system should employ functions to ensure the data is untampered and accurate. Finally, if a system is not available, then this can create additional risks for a company, which is why the systems should provide safeguards to provide access for authorized users to the data and system resources when they need it.

Like other IT systems, there are some similar components found in the security system, and we can apply the security capabilities in a similar fashion. In a typical security network, the components which should be secured are the endpoint devices, the network, and the data.

When addressing endpoint security, we need to look at devices such as cameras, recorders, and workstations. Each of these points represents a means to access the overall security system. The first line of defense for these devices should be implementing strong passwords and disabling default user accounts. Next, these devices should be regularly updated. While updates for cameras, recorders, and workstations may provide new functionality, they will often include fixes to known vulnerabilities found in these systems or implement new security functionalities. Additionally, many devices come enabled with a host of services that can be used by the customer. If these services are not used, then they should be disabled to minimize exposure on the network. Finally, logging of the endpoint devices and regular audits can reveal unexpected behavior or potential vulnerabilities in these devices.

As we move from the endpoint to the network, we need to identify how we can fortify the security network from cyber threats. The biggest concern with network security is access. Network resources, such as switches and routers, should be located in secure spaces where physical access is controlled. Further, if the system architecture permits the security system should be isolated from the corporate network. Segmentation can be achieved either by physically isolating the networks or by segmenting them through Virtual LANs. There are even technologies such as MAC filtering or 802.1X, which will only allow access to authorized devices.

Finally, to protect the data within the security system, we can take the following steps. First, defining user access to the system data is critical. Even though user access to the system may be controlled, when watching the video, users may use a personal electronic device to capture the data displayed on their screen. Implementing a "no personal electronic device" policy will further protect from data breaches. In the event data needs to be exported from the system, it should be done in an encrypted method. This safety measure ensures the data remains protected, and only an authorized user can decrypt the data for use.

Securing your security system should be a top priority, and it can be achieved with planning and proper implementation. Even with this, the system should be reviewed regularly to ensure the latest patches are applied, the security plan is in place and operational, and any new equipment or system integrating with the system meets the minimum standards in place for your system. These simple steps will help in maintaining your cybersecurity.

Copyright ©2019 1105 Media Inc. All rights reserved.

SALIENT™