News

Hardware Cybersecurity: Insights

Our comprehension of cybersecurity is based around the global internet, where software attacks threaten our working days and everyday lives. We fail to relate cybersecurity to the threat to autonomous computer networks. A third party physically breaks into a system via its infrastructure devices.

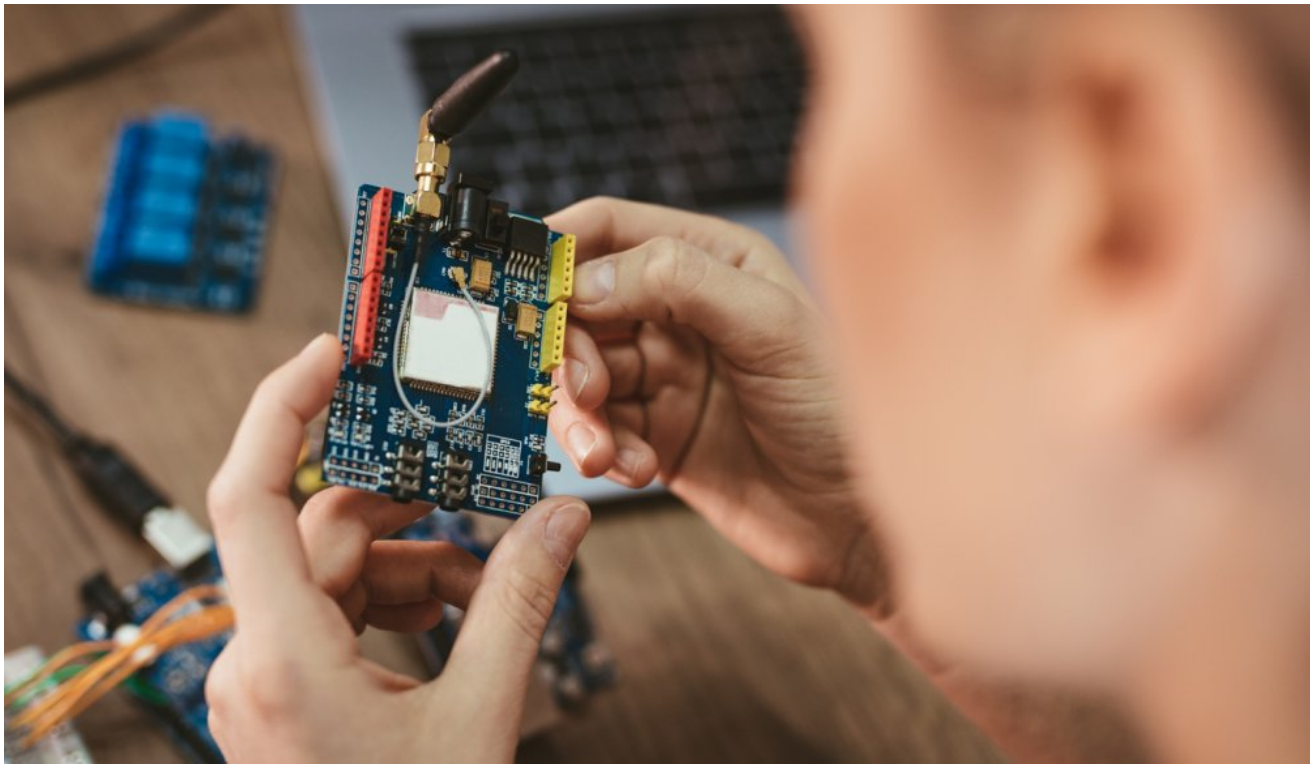
Due to their nature, IP security and surveillance networks put physical network connections in secure and unsecured locations. Vulnerable positioning provides ample opportunities for the would-be attacker, so due care and attention must be paid to equipment protection. However, installers must also treat secure sites in exactly the same way. The point of attack could originate from a source fully entitled to be within an area. No chances can be taken.

An Ethernet network comprises both active and passive equipment. [(1)] The active

equipment includes Ethernet switches [2] and media converters. The passive, a combination of cables, connectors, and management such as cabinets might also include additional active equipment, such as environmental conditioning and monitoring systems.

The security threat to the network at this level results from a third party physically connecting to the active network devices, or by removing an edge device from the network and attaching unauthorized equipment in its place. The connection could be to an optical port, but that would require the third party to have the correct optical interface, so, for opportunistic reasons, it tends to be a connection via an electrical interface. Electrical Ethernet ports are based around an industry standard, so connecting to these is relatively simple. Every laptop today has such a connection, the probable weapon of attack is readily available.

Active Equipment Defense



Ethernet switches are available in managed or unmanaged forms. The managed platform has many more features and allows the user to configure and remotely monitor the device. The unmanaged unit has no such facilities. It simply does the basic job based on its shipped configuration. Media converters tend to be in an unmanaged format only. Where security is concerned, managed units offer several facilities to prevent unauthorized entry to the network. In contrast, unmanaged forms do not. Thus managed Ethernet switches

should be used throughout your network.

It tends to be the case that the most straightforward features offer the best security, and with Ethernet managed switches, that persists. The ability to disable a switch port that's not being used in the current network configuration, through the management interface, might seem an obvious security feature. Still, it is one that a lot of network operators fail to employ and may not even know exists on their devices. As you can imagine, the rules are straightforward: if the port is not being used, then disable it, so no unwarranted party can plug directly into your network. If the port needs to be used for legitimate traffic in the future, simply open it via the management system. And while we're talking about the simplest features being the best, the default username and password that every managed Ethernet switch is shipped with, to enable you to gain access, should be changed to a username and password, commensurate with your security policy. There is no point in applying all this security if it could be changed by our attacker connecting to the comms port (3) of the switch and gaining access simply by reading the manual!

Once a link has been established between two active units in the network, a LINK acknowledgment (normally an LED indication) is generated and dropped immediately. The link is broken. This simple Layer 1 hardware-based trigger has been utilized by ComNet in their unique Port Guardian feature. It can be used to shut a port down on the basis that a loss of link is a potential attack. The feature can be further expanded to shut down ports in the event that power is lost to the active device - just in case our attacker has the smart idea of switching connections once the switch is powered down. Suppose any units are deployed in unsecured locations. In that case, the port receiving communications from that site should be activated with this feature to counter link breaks in these areas.

Passive Equipment Security

Security should be applied to the passive components of the network as well as the active ones. How many times have you walked along the pavement and observed the door of a utility company street cabinet hanging off, or even the access flap open on a lamppost? The reason is that, for most cases, the system owner or operator has no idea that the door of their cabinet is open, and their system is not secure! If any part of the network is housed within an enclosure, some sensor form must be on the door to tell you if it is open or closed. Suppose the door is open, and you are not aware of it. In that case, you provide an easy target for any attacker and, at the same time, allow the elements to damage your enclosed equipment. And remember, it doesn't just need to be active equipment. If the enclosure simply houses cable management, that could be an opportunity to break into the network. This requirement is an absolute must in unsecured locations!

Conclusion

To guard against attacks, managed Ethernet switches should always be used as the network's active building blocks as they offer the maximum level of security when configured correctly. Managed units will also provide users with the ability to remotely control and monitor network devices. They will generate automatic warning signals if an issue arises. Any managed Ethernet switch must be configured based on the site's security levels and operational requirements to ensure correct operation.

Those who ignore the basics of network security and opt instead for cheaper, unmanaged devices expose their networks to the risk of hackers. Hackers who can very quickly turn a sophisticated security network to their own advantage. And with the safety and protection of critical infrastructure, data, and communications at stake, are you prepared to take that risk? / it seems an irresponsible risk to take.