Net2 - Network Security Recommendations

Overview

In order for your Paxton Net2 system to be as secure as it can be on your site, Paxton recommends that the installer (or IT department) implement IT security mechanisms best practice at each of the 7 layers of Network Open Systems Interconnection (OSI) model.

Implement strong physical security

Implement strong physical security to company premises such as by using Biometrics, token-based authentication, etc. so that an outsider can be stopped before he/she can enter a building with a corporate network.

Implement Network Access Control standards such as IEEE 802.1X authentication for securing LAN and WLAN

This standard enforces security policy by granting only security policy–compliant devices access to network assets when those devices are plugged into a physical LAN port or are connected to a WLAN SSID. This standard not only handles access authentication and authorization functions but even control the data accessed by those specific users by recognizing users, their devices and their network roles. IEE 802.1X is natively supported by all Windows, Mac and Linux machines

Implement next generation Firewalls to prevent external and internal attacks

Implement a next generation firewall which, in addition to traditional packet based stateful inspection, also performs application layer inspection, intrusion prevention and detection, securing web traffic, etc.

Furthermore, stretch any potentially insecure internal layer 2 VLANs to the firewall and protect access from those VLANs to other trusted/secure VLANs using configurable security policies.

Implement VLANs (Virtual Local Area Networks) for network security and segregation

VLANs allow us to keep data packets from multiple networks (such as departmental networks, critical server networks, etc.) separated. Network segmentation with VLANs creates a collection of isolated networks within a corporate network and reduces the attack surfaces because even if an outsider gets access to a small logical network, he/she won't be able to view or directly attack devices on other VLANs.

Implement strong passwords for Net2 Server application authentication and associated databases