Physical Access Control System Security Checklist

This checklist is designed to provide guidance in hardening the physical access control system (PACS) environment from network and computer-based attacks. The majority of checks are to be performed on the organization's internal network and may require assistance from network and server support personnel. Additional checks for credentials (access cards, fobs, etc) and credential readers are also included.

Access control server

- **Hostname/DNS entries**
  - Avoid obvious names for the server, such as CCURE or AMAG. This naming convention provides attackers with a shortcut to locating the access control server.
  - Ensure hostnames and DNS entries to not include the manufacturer name, physical access, or PACS.
- **Web Interface**
  - Disable the web interface if not required
  - If disabling the web interface is not an option
    - Limit the IP addresses that can access to Physical Security personnel it via network filtering
    - Enable secure socket layer (SSL) or transport security layer (TLS) and obtain a valid security certificate from a recognized security authority.
  - Require all personnel to have an individual account on the PACS server (even to contract guard staff).
- **Database** - Smaller PACS implementations may host the database on the access control server. In larger installations, it may be hosted on a separate server.
  - Ensure that accounts with blank passwords are not present
  - Ensure that vendor required machine accounts have a strong password. Set a strong password containing special characters, numbers, upper and lowercase letters
    - Prohibit the use of company name or abbreviation, street addresses, or phone numbers.
  - Ensure that database backups are encrypted
  - If possible, data in the database itself should be encrypted.
- **PACS Software**
  - Enable active directory authentication for all users (if supported)
  - Verify that individual accounts have proper access rights
    - Read only
    - Create/delete employees
    - Create/delete groups
    - Create/delete card formats
    - Delete event log files
  - Enable logging for all events
- **Who can over-ride the PACS**
  - Are there senior managers or emergency responders who can over-ride the PACS? How is their access controlled?

    - Ensure that office cleaning staff access the PACS as individuals, not via a generic access card.
- **If the client resides in multi-tenant space, identify**
    - Does the Building Management company have over-ride access over the PACS for tenant controls
    - How do Building Management staff (HVAC staff, maintenance staff, etc.) enter the tenant space (special cards, hard keys, etc.)

Access control panels

Also known as door controllers, these are often scattered throughout the network and may not all reside on the same virtual local area network (VLAN). The access control panels can be sensitive to intense port scanning on the network side. Safest assessment method is to review documentation for the following items and manually verify their presence.

- **Onboard diagnostic web servers**
    - Most commonly found on port 80 and 443 (Internet Explorer is required for most products)
    - Disable web server if not required
    - If disabling the web interface is not an option
        - Limit the IP addresses that can access to Physical Security personnel it via network filtering
        - Enabled secure socket layer (SSL) or transport security layer (TLS) and obtain a valid security certificate from a recognized security authority.
- **Insecure access protocols**
    - Disable SNMP if not required.
    - If disabling SNMP is not an option
        - Set a strong community string containing special characters, numbers, upper and lowercase letters
        - Prohibit the use of company name or abbreviation, street addresses, or phone numbers.
    - Disable FTP access
    - If disabling FTP access is not an option
        - Do not use anonymous FTP
        - Set a strong password containing special characters, numbers, upper and lowercase letters
        - Prohibit the use of company name or abbreviation, street addresses, or phone numbers.
        - Require password reset every 60-90 days
    - Disable telnet access
- **Network access**
    - Restrict network access to physical access machines only
    - Limit the IP addresses that can access it via network filtering

Guard workstations

These workstations are often in public areas and not staffed 24/7, which makes them prime for physical attacks.

- The workstations should be in a locked computer cabinet.
- The workstation should not also used as the guard's primary computer for accessing email and the Internet.
- Autorun should be disabled on USB and DVD drives
- Local administrative rights should be disabled on the workstation
- Monitors should be equipped with privacy screens to prevent shoulder surfing
- Ensure that all users have individual accounts on the workstation with a strong password

Credential-issuing machines

- The machines should be located in a non-public area
- The machine should not also used as the operator's primary computer for accessing email
- Autorun should be disabled on USB drives
- Monitors should be equipped with privacy screens
- These machines should not have Internet access
- All personnel should be required to have an individual account with a strong password

Access card and facility code numbers

- Access card/facility code numbers should never be stored outside of the PACS. They should not be included in the following:
  - Email
  - Work tickets or logs
  - SharePoint or other documentation portals
- Access card/facility code numbers should **never** be printed on a credential (access card, electronic fob, mobile device)
- If system logs contain card/facility code numbers, these logs should not be stored in clear-text

Credential

- Determine manufacturer and model number in order to research current vulnerabilities and exploits
- Evaluate physical appearance
  - Are card or order numbers present?
  - Is the vendor logo displayed?
  - Is hologram present?
- Employees should be issued an RFID blocking cardholder for their access card

Credential readers

- Evaluate physical appearance – readers should be non-apparent and tamper-evident
  - Are readers visible from the exterior perimeter?
  - Are readers pictured in "street view" portions of Google and Bing maps?
  - Is anti-tamper tape installed on readers?
  - Are reader wires fully potted?
  - Are readers installed with security screws
  - Is the anti-tamper feature enabled?

Company website

- Credential readers should not be pictured on the company website
- If organization is located in a leased facility are credential readers pictured on the leasing company's website?
- Are access cards displayed in photos on company website or social media?

Shodan

- Are PACS components cataloged in Shodan?

Vendor access

- Are vendors required to connect to the PACS via a VPN?
    - Does the VPN require multi-factor authentication?

To learn more about our Physical Security Consulting services, please call us at (703) 914-2780 or email info@securicon.com.