Defense in Depth Documentation for Perimeter Breach at Secure Facility in Washington DC

Michael Huber

https://nvd.nist.gov/800-53/Rev4/control/PE-3

The following list below is a summarized version of the National Institute of Standards Technology (NIST) guidelines. Particularly to secure the construction of and implementation of all possible physical security issues or concerns. Going through NIST Special Publication section 53 there are many concerns to be had and NIST SP 800-53 has the answers to many. Moving through 800-53, Information access to enforce physical access authorizations to the system is needed around the building at all access points and especially sensitive information systems areas and rooms, such as server rooms, media storage areas, and data centers. There must be security checks at every entrance to identify people and search belongings before moving through the building. Guards and alarms are needed to monitor and prevent the intrusion of unauthorized access. Lock and Secure all unused devices that can access the information systems. Deploy safety nets to stop or alert any unauthorized access that would get through any security with tamper protection devices, software, and hardware. Lastly perform surprise penetration testing to see how well the security implemented works in real time.

Physical Access Control & Security Basics and Methods Based off NIST SP 800-53

- INFORMATION SYSTEM ACCESS: Enforce physical access authorizations to the information system in addition to the physical access controls for the facility
    - Server rooms, media storage areas, data and communications centers
- FACILITY / INFORMATION SYSTEM BOUNDARIES: Perform security checks at the boundary or perimeter of the building checking for unauthorized access or infiltration of information or removal of information system components
    - Determine the extent, frequency and/or randomness of security checks to adequately mitigate risk associated with exfiltration
- CONTINUOUS GUARDS / ALARMS / MONITORING: Employ guards and/or alarms to monitor every physical access point to the facility where the information system is held
- LOCKABLE CASINGS: Use lockable physical casings to protect the information system and its components from unauthorized access
- TAMPER PROTECTION: Employ safeguards and fallbacks to detect and prevent physical tampering or alteration of hardware in the information system
    - Tamper detection and prevention can employ many types of anti-tamper technology like, tamper-detection sesals and anti-temper coatings as well as software programs to detect hardware alterations through counterfeiting and other supply chain-related risks
- FACILITY PENETRATION TESTING: Employ unannounced and surprise penetration tests attempting to bypass or circumvent security controls associated with physical access points around the building

Listed below are ways and examples for us to protect the information system and its contents by following and properly implementing these devices and techniques. Using keys for wireless access, locks and keys to doorways and secure rooms, keypads, biometric scanners, two factor authentication, ease of use techniques such as cable and power management. These are examples for which devices and techniques can be used to prevent any unauthorized access or any unforeseen incidents such as undodgeable or must be mitigated risks, like weather or power outages.

Physical Protection/Monitoring

- Secure keys, combinations and other physical access devices.
- Protect inventories such as organization-defined physical access devices.
- Change the combinations of locks and keys when they are lost, compromised, or when individuals are transferred or terminated.
- Monitoring physical access to the facility where the information system resides to detect and respond to physical security incidents.
- Review physical access logs
- Facilitating the user access list by deleting or adding facility when access is no longer required for an individual.

Cable Management

- Employ redundant power cabling paths that are physically separated by.
    - Automatic voltage controls

Power Management

- Provide a long-term alternate power supply for the information system in the event of an extended loss of the primary power source.
    - Self-contained
    - Not reliant on external utility power generation
    - Capable of maintaining in the event of an extended loss.

Environmental Events:

- Employs and maintains automatic emergency lightning for the information system that activates in the event of a power outage or disruption that covers exits and evacuation routes.
- Employs and maintains fire suppression and detection devices/systems for the information system that are supported by independent energy source.
    - Notifies responders in the event of a fire
    - Undergoes inspections from qualified inspectors
- Maintain/Monitor temperature and humidity levels where the information system resides
- Employ automated mechanisms to detect the presence of water in the vicinity of the information systems.
- Ensures information system components are protected in with national emissions and policies and procedures based on the security category.

In the list below are the ways and examples that we are going to implement each security measure to prevent any unauthorized access to the information systems. Using most of these we should be able to safely secure all of our assets without any hitches or unforeseen risks, other than the ones that cannot be dodged or prevented. Using ID badges, timers and lockouts, as well as personal keys and pass codes or passwords for each individual employee that is required to change after a certain time. Using as much biometrics as we can without it being replicated. All of this is needed to properly secure our building and systems within.

Safe Encryption Security for Organizational Members

- Enforce biometric controls at all secure points of entry to the building with added two-factor authentication such as a 4 digit numeric PIN and/or 4 digit alphanumeric passcode with 128-bit encryption
- Using ID badges, set up system to track every ping to enter the building
- Place cameras and monitoring controls at every main and secondary point of entry and egress that send video and audio to security system hub for monitoring
- Place access controls on all points of entry and egress
- During emergencies when exits are meant to be unlocked, stagger all points of egress for 60 seconds until they are unlocked
- Set off site and onsite controls to lock down all points of entry and egress, as well as all sensitive offices and portions internally within the building
- All employees are subject to security credential analysis on a bi-monthly basis
- All contractors are subject to security credential analysis on a monthly basis
- 3 failed attempts to access building using legitimate or illegitimate credentials results in lockdown of point of entry where failed attempts occurred
- If building is attempted to be accessed at three different points and all attempts fail within 15 minute period, all points of entry and egress to building are locked down
- Onsite security at all major points of entry with ability to enact or lift lockdown protocols at all points of entry and egress
- Remote security inside building that can enact or lift lockdown protocols at all points of entry and egress
- Facial and voice recognition software to analyze all camera monitors in building
- Audio and Video monitoring at all emergency exits, fire alarms, or other methods of declaring emergencies within the building
- Access controls to networks require individual 256-bit encrypted key that is different for each information systems employee
- All encryption keys, passwords, and individual employee credentials must be updated every 90 days with no repeats within a 365 day period
- 40-bit, 104-bit or 128-bit encryption on all wireless networks, depending on legacy and bandwidth restrictions
- System Administrators must have redundant system administrators' approval before any changes are made to the overall system
- All lower employees must seek at least two system administrators' approval before making any changes to any system

- Daily redundant backups of each individual system
- Backup default system image for each system in building must be able to be enacted onsite and remotely in case of corruption errors in OS
- Security of all routers, switches, modems, and access points must be enacted at all times and at all levels
- Access control of all ports, switches, routers, information systems must be able to be accessed both onsite and remotely, and be able to be reset and controlled at the most fundamental levels
- Only authorized employees and system administrators are able to access system security settings and controls
- Access to all security settings within each system require authorized and encrypted access controls which are unique and must be updated every 90 days
- Intrusion Prevention Systems, Firewalls, Port and network access security and all software and hardware protection systems must be active at all times
- All protection hardware, software, and protocols must have both redundant and inverse duality within each information and security system

The organization:

- Enforces physical access authorizations at [Assignment: organization-defined entry/exit points to the facility where the information system resides] by;
    - Verifying individual access authorizations before granting access to the facility; and
    - Controlling ingress/egress to the facility using [Selection (one or more): [Assignment: organization-defined physical access control systems/devices]; guards];
- Maintains physical access audit logs for [Assignment: organization-defined entry/exit points];
- Provides [Assignment: organization-defined security safeguards] to control access to areas within the facility officially designated as publicly accessible;
- Escort visitors and monitors visitor activity [Assignment: organization-defined circumstances requiring visitor escorts and monitoring];
- Secures keys, combinations, and other physical access devices;
- Inventories [Assignment: organization-defined physical access devices] every [Assignment: organization-defined frequency]; and
- Changes combinations and keys [Assignment: organization-defined frequency] and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.

More techniques that are going to be used to protect our information system if unauthorized access is accidentally or purposefully given to outside intruders. Using timeouts and encryption as well as authentication methods and key management techniques we will have little to no problem maintaining our Information system. Protecting our WLAN and APs we will prevent unauthorized access to the network from outside threats and secure data exchanges will ultimately protect our information system and the information within

Wireless and Information System Security Concepts

- Establish Security Policies
    - Confidentiality and integrity protocols for protecting unicast traffic
    - Authentication method for mutual authentication of the AP and AS
    - Cryptographic key management approach
    - Pre-authentication capabilities
- Key Generation and Distribution
    - Ensure security association keys are new
    - Distributing group key for multicast and broadcast traffic protection
    - Message integrity checking, to protect against tampering and to validate the source of traffic
    - Message encryption, to protect against unauthorized disclosure of data
- Protected Data Exchange
- Connection Timeouts and Termination
    - Automatically time out and sign out unused computers and and stop data leaking or accessing the internet until powered back on or in use again
        - Must re-enter credentials and login information when back in use
- WLAN Security Practices
    - Initiation of tasks that an organization should perform before it starts to design WLAN solutions
    - Acquisition/Development phase split into Planning and Design, and Procurement
    - Implementation of WLAN security into the system without causing errors or downtime during merge
        - Test on disconnected network before implementation
    - Operations/Maintenance of the network
    - Disposition encompassing tasks that occur after a system or its components have been retired