CCCO State Security Center Recommendations for LACCD

#	Category	Details
1.	Patch Computer Systems	Patch all Critical and High Vulnerabilities found in this report as soon as possible or put in place other controls to mitigate these risks.
2.	Patch Computer Systems	Medium vulnerabilities should be reviewed and prioritized to patch, fix or accepted as a reasonable risk.
3.	Replace Old Computer Systems	Migrate all applications that require XP and Server 2003 to operating systems that are under support, or enact further controls to isolate and protect these systems.
4.	Automate Vulnerability Scanning	Implement a Vulnerability Management product such as Tenable Security Center. Security Center is available free of charge from the CCC Security Center. Vulnerability Management systems scan your network to find vulnerabilities and alert you. It is recommended that weekly credentialed scans be set up for all systems. Credentialed systems log onto the systems and find out of date software that isn't visible from the network such as old versions of Flash and Acrobat Reader.
5.	Retire Old Protocols	Disable LLMNR on all workstations and servers, instructions can be found at https://www.cccsecuritycenter.org/remediation/llmnr-nbt-ns
6.	Retire Old Protocols	WPAD should be disabled on all workstations and servers, or a WPAD DNS entry should be created.
7.	Increase Password Complexity and Password Security	While we did not use the pass the hash attack method, steps should be taken to prevent it use. Instructions for remediation can be found at https://www.cccsecuritycenter.org/remediation/pass-the-hash
8.	Increase Password Complexity and Password Security	Password entropy needs to be increased, with the default password policy of 8 characters attackers can easily crack any password hash within 48 hours using commodity Graphics cards and an open-source program called Hashcat. Longer passphrases that a user can remember are general thought to be better than mandating lots of special characters. For sensitive passwords such as domain admins passwords should be at least 16 characters long, for users passwords should be at least 12 characters long. Users should be educated on how to create a passphrase that is secure and easily remembered.
9.	Increase Network Segmentation	Segregate the network and add a management network only available to IT staff. Many remote access servers were found including HP System Management, network and SAN switches, and ESXi consoles. These services should only be made available to IT Systems Administrator as a vulnerability in these can lead to complete control of the system.
10.	Increase Password Complexity and Security	All remote administrative access should be using two factor authentication and should not be available directly from the internet. A VPN should be used for servers that need to be remotely administered from outside the internal LACCD network.

11.	Increase Network Segmentation	Printers and security cameras should also not be available to the general users on the network. The Eyewitness reports in the raw data of this report found printers and several security cameras. Best practice is to have the printers in a separate VLAN only accessible to a print server. Direct access can both allow students to print LACCD Vulnerability Assessment Report for free, as well as send non-desirable files to be printed. A recent example would be a person sent Nazi propaganda to every printer that was directly connected to the internet. Security cameras access should also be restricted to only those who need access.
12.	Deploy Security Incident Event Management Technology (SPLUNK)	Implement a SIEM system to correlate and analyze all of the systems logs. The CCC Security Center offers ten gigs per day of free Splunk core indexing.
13.	Increase Security of Web Servers	For web servers that contain and transmit secure information such as passwords, legitimate SSL certificates should be installed on them. Free and unlimited SSL certificates can be obtained by signing up for the InCommon membership offered by the CCC Technology Center.
14.	Standardize Security Control	All colleges should start implementing the CIS Critical controls, as well as two-factor authentication to access systems that contain sensitive data such as Social Security Numbers. These were included in the State of California's most recent Data Breach Report https://oag.ca.gov/breachreport2016 as being the reasonable set of security controls for organizations collecting and storing private information. It is the opinion of the CCC Security Center that not implementing these could result in the risk of further liability in the case of a data breach.

The detailed report is available onsite for the visiting team.