Operation DEV

S-Mart Network & Security Evaluation

4/29/2019

S-Mart Network & Security Evaluation

This document contains a summary of issues detected during S-Marts network & security assessment test. We found numerous vulnerabilities in the network & security system. This assessment will identify any necessary changes to the system. S-Mart needs to make critical changes to compete with bigger companies. The overall issue score grades the level of danger in S-Marts current network & security plan.

Current Network & Hardware Configuration:

Currently S-Mart is running off Windows XP, which is no longer supported by Windows. This means windows will no longer offer security patches. This is devastating to S-Marts network. Leaving computers running Windows XP vulnerable to attack. The goal is to launch new machines with Windows 10. S-Mart is currently using a bus network topology. The bus topology connects each node to a single cable. Some connector connects each computer or server to the bus cable. Our proposed new network topology will resemble a star topology. This will help S-Mart avoid disruptions to the network when connecting or removing devices. The new topology will make it easy to detect faults and to remove parts during the first few months of the grand opening.

Current Security & Software Configuration:

Currently S-Mart has outdated security protocols S-Mart is using TLS version 1.0, which has been discontinued as of June 30th 2018. The TLS 1.0/1.1 and Secure Sockets Layer 2.0/3.0 protocols are deprecated and provide insufficient cryptography for securely transmitting data. S-Mart will be upgrading to TLS version 2.0. Making this change in the network will help provide better security for virtual payment terminals, Back-office servers, Web/application servers.

New Proposed Network & Hardware Configuration:

New Proposed Software Configuration:

Security Test 1

Potential Password Strength Risks:

Issue: There were 16 local account passwords that did not meet the current security standards. Weak passwords on local accounts can allow a hacker to compromise the system. Weak passwords can also lead to the spread of malicious software that can cause business and productivity affecting issues. Now is the time to identify the smaller problems that ultimately can damage S-Marts new vision.



Solution: S-Mart will inherit the following password protocols. Password composition rules require the inclusion of 3 of the 4 following character sets: lowercase letters, uppercase letters, numerals and special characters. Allowable special characters are ~#$%^&\*()\_+|`-=\{}[]:”;’<>?,./ and the space character (depending on system support). Passwords may not include words of more than 4 characters, as tested against a dictionary of at least 50,000 words.

For all policy levels, the selection of a passphrase of at least 18 characters eliminates the password composition rules and dictionary check. Passphrases are subject to minimal tests to prevent use of common or trivial phrases.

Two-Factor Authentication is required for policy level P6 and optional for all faculty, staff and affiliates. Faculty, staff and affiliates whose accounts are compromised will be required to enroll in Two-Factor Authentication.

Unsupported Operating Systems:

Issue: All computers onsite were found using an operating system that are no longer is supported by new security protocols. Unsupported operating systems will never receive vital security patches. This is a huge security risk to the company and needs to be updated before the system is compromised.



Solution:

S-Mart will replace all computer with updated Dell Inspiron 24 3000 All-in-One Desktop. These machines feature Windows 10 Home 64bit English, Up to 7th Generation AMD A9-9425 Processor with Radeon R5 Graphics, Up to 256GB M.2 Solid State Drive. Machines are scheduled to be ordered May 1st.

Anti-spyware not installed: Anti-virus not installed:

Issue: Anti-virus software was not detected on 9 computers. Without adequate anti-virus and anti-spyware protection on all workstations and servers, the risk of acquiring malicious software is significant.



Solution: To avoid both security and productivity issues, we strongly recommend S-Mart deploys new software immediately. This a level 10 security issue and will be highlighted as dangerous. Every S-Mart branch will upgrade to windows defender May 1st 2019. Windows defender features the following:

Virus protection and removal

Virus protection and removal Checkmark icon

Malware protection and removal

Malware protection and removal Checkmark icon

Spyware detection and removal

Spyware detection and removal Checkmark icon

Boot-time protection

Boot-time protection Checkmark icon

Real-time protection

Real-time protection Checkmark icon

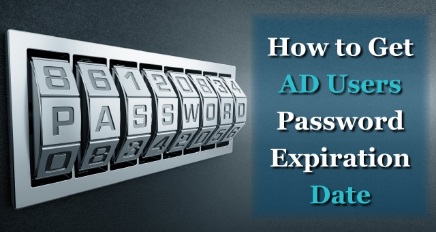
Cloud-based protection

Cloud-based protection Checkmark icon

Network inspection

User Password set to never expire:

Issue: S-marts accounts with passwords set to never expire present a risk of use by authorized users. They are more easily compromised than passwords that are routinely changed. S-Mart needs to implement this new protocol to have passwords expire after 30-90 days.



Solution: S-Mart must manage password expiration with updated password policies.

Step 1: Investigate all accounts with passwords set to never expire and configure them to expire regularly.

Step 2: Set **maximum password age** to a value between 30 and 90 days, depending on your environment. This way, an attacker has a limited amount of time in which to compromise a user's password and have access to your network resources.

Step 3: Set passwords to expire after a number of days between 1 and 999, or you can specify that passwords never expire by setting the number of days to 0.

Potential Disk Space Issue:

Issue: Computers were found with significantly low free disk space. S-Mart plans on replacing all machines in S-Marts network during the implementation of the new plan. Each new machine will have new updates on a monthly basis. S-Mart plans to use Windows 10, because Windows creates the low disk space warning to alert when users are running low on space. It is vital to have an adequate amount of available storage space  
on your hard drive because programs might fail due to an inability to  
allocate space.



Solution: Free or add additional disk space for the specified drives. S- Mart will run the following monthly machine updates:

Step 1: Disk Clean-up is Windows’ built-in tool for removing unnecessary old files Recycle Bin, Temp folders, and other random system files are potentially hogging gigabytes of free space – and it’s safe to delete those files.

Step 2: Uninstall Unnecessary Applications

Step 3: Reduce Space used for system restore

User has not logged in in 30 days

Issue: S-Mart users that have not logged in in 30 days could be from a former employee or vendor and should be disabled or removed. Recommendation: Disable or remove user accounts for users that have not logged in in 30 days. S-Mart is currently using POP3 which has no logging in limits. S-Marts plans on switching to SMTP protocol. SMTP uses maintenance settings to limit the amount of log data on the server by age or by directory size.



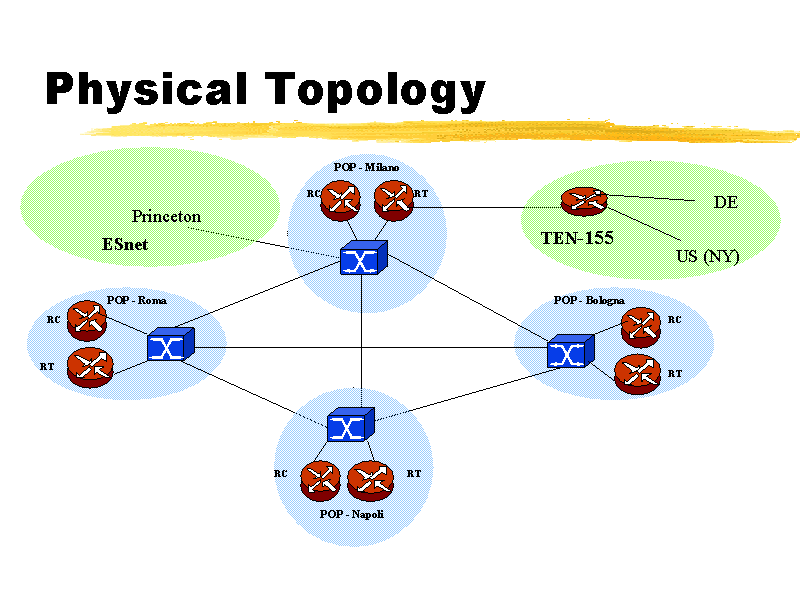
Solution:

1. Configure the log file location to a dedicated volume that won't impact the server if it runs out of disk space.
2. Use a scheduled task to run a script that removes files older than a specified number of days. There are PowerShell scripts that can easily be found on various blogs and community sites for this.

Network Test 1

Issue: Physical Topology

Solution: Develop network design plan to incorporate a fault tolerant network topology that meets network downtime requirements and provides redundancy to critical assets.



Issue: Switch Selection

Solution: Develop migration plan to replace switches on the network that do not meet IACS standard requirements such as unmanaged switches.



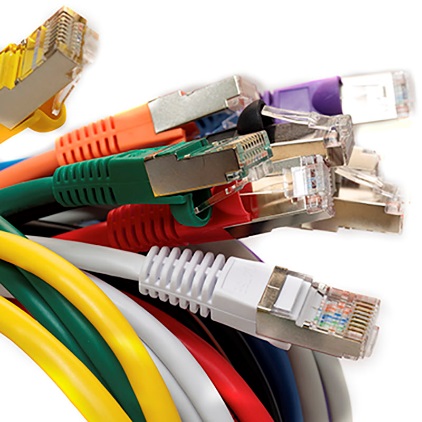
Issue: Environmental Conditions

Solution: Network devices may be compromised due to environmental conditions. Immediate evaluation all network devices is needed and replacement of environmentally degraded equipment is recommended.



Issue: Cable Selection

Solution: Evaluate cables and connectors being used and consider plan for upgrading cable infrastructure.



Issue Cable Management

Solution: Develop cable management standards for enclosures and where excess cable exists. Any cables that have not been managed to meet specifications require cable testing so any damaged cables can be identified.

