विद्ययेव संवर्धनम् ।

UNIVERSITY OF MORATUWA

Week Six at Pandora Company Limited

Bridging the Islands of Systems Chaos

Name : Lahiru Randika **Index : 210527J**

1. Introduction

At present, Pandora Company Limited employs a decentralized management system, which covers 25 standalone Windows computers, thus exposing the company to cyber security threats and ineffective management of the systems. Each PC has its own setup, resulting in a lack of uniformity concerning user policies, password policies, software installations, and security configurations. This document addresses the issues that come with the management of personal computers in a decentralized manner and suggests migration to a more centralized management. It also gives a tip-to-tip recommendation on how to move to a single management system which will promote security, efficiency in operations, and overall effectiveness.

2. Unified Management Exploration

A decentralized environment in which each computer is managed on its own will undoubtedly come with various cybersecurity concerns and operational risks. The absence of standardized policies for users, security settings, or operating systems updates can result in high-profile security incidents and other complications.

Cybersecurity Challenges and Risks

- **Weak Passwords:** The use of passwords such as ‘1234’ by employees is a serious security loophole. Weak passwords can be guessed or hacked, and this poses a threat to security.
- **Inconsistent Security Configurations:** In the absence of a centralized control system, PCs may be configured with different firewalls, antivirus, and encryption configurations. This configuration inconsistency creates a window for cyber-attacks as some systems are protected while others are left bare.
- **Difficulty in Deploying Updates:** Uniform deployment of patches and updates becomes impossible in a decentralized architecture. It is likely that some PCs will be updated while others are not, therefore exposing the latter to known vulnerabilities.
- **Access Control Issues:** Inappropriate, inconsistent or no access control means that employees may have the ability to retrieve information classified as sensitive whether by design or by mistake.
- **Human Error and Configuration Drift:** The PCs and their configurations tend to become unmanageable over time as they stop being kept in accordance with an organization’s policies.

Proposed Enterprise Solution: Microsoft Active Directory

To mitigate these issues, it is advisable that the Pandora Company implement Microsoft Active Directory (AD) as its primary management platform. Active Directory (AD) provides the benefits of administrative power over users, computers, and policies regarding security. Its main functionalities are concerned with policies such as:

- **Password Policies:** Ensures the entire organization adheres to rules on password complexity, the rate of expiration, and the freezing of accounts.
- **Group Policies:** This feature of AD Group Policy facilitates the administrator in installing applications

- **Centralized Update Management**: Coupled with **Windows Server Update Services (WSUS)** or **Microsoft Intune**, updates can be deployed and managed centrally, ensuring that all computers are patched simultaneously.
- **Access Control**: Role-based access control (RBAC) can restrict access to sensitive files and systems, ensuring that only authorized people can access specific resources.

3. Advantages & Benefits Analysis

Transitioning to a centralized user/system management approach offers several direct and indirect advantages, which will enhance Pandora's security and operational efficiency.

Immediate Advantages

- **Better Security:** It is easier to ensure that security measures are universally applied, thus minimizing the chances of any violation occurring are minimized. Measures such as limiting access through password schemes and access permissions coupled with automatic installation of updates enhance security by preventing access to users who do not qualify.
- **System Homogeneity:** Group policies ensure that all systems adhere to the same configuration, reducing the risk of misconfiguration or overlooked security settings.
- **Management Efficiency:** All computers can be managed via a single interface, eliminating the need for repetitious processes like installing, upgrading, or fixing problems on the computers.
- **Compliance is Made Easy:** One of the systems enables the standardization of protective measures and all changes made within this system are recorded within the system making compliance enforcement less of a task.
- **Improved Scalability:** A centralized system can easily accommodate future growth by adding new users or devices without disrupting existing configurations, making it easier to expand the IT infrastructure as the company grows.

Secondary Benefits

- **Enhanced Efficiency:** There will also be less downtime experienced by employees due to the uniform applications and configurations available and enabled.
- **Better Management of IT:** The functional areas are improved as IT activities are not spent on routine actions like patching, installing, or configuring systems, but done with other strategic objectives of the organization.
- **Faster Incident Management:** For example, when a security event occurs since all activities are recorded in one place and there is a tool like Microsoft Defender for Endpoint, it is easier to mitigate and manage the various threats in a shorter period.
- **Cost Efficiency:** A centralized user management system reduces the risk of data breaches and compliance penalties while cutting support costs by standardizing systems. Consistent security enforcement and automation minimize the chances of expensive security incidents and the financial impact they can cause.

4. Recommendation Report and Steps

Recommendations:

To transition from a decentralized to a centralized system, Pandora Company Limited should implement Microsoft Active Directory (AD) for managing user access, enforcing security policies, and streamlining IT operations. Start by auditing all 25 PCs to document current setups, then install AD on a Windows Server. Create Organizational Units (OUs) aligned with departments for easier management.

Enforce strong password policies and role-based access control (RBAC) to secure access and implement multi-factor authentication (MFA). Use centralized update management tools like WSUS or Microsoft Intune to ensure uniform patching across all systems. Leverage Group Policy to standardize security settings and automate software installations.

Provide employee training to ease the transition and ensure adherence to new security protocols. Monitor the system with Microsoft Defender for Endpoint and adjust policies as needed. Regular system audits should be conducted to maintain compliance and improve overall security.

Steps to follow:

Step 1: Conduct an Initial Audit

Before transitioning, perform a full audit of the existing PCs, documenting current user accounts, software installations, and security configurations. This will help identify gaps and inform the design of the new centralized system.

Step 2: Set Up Microsoft Active Directory (AD)

Implement a Windows Server to host the AD infrastructure. Install and configure AD and create Organizational Units (OUs) that align with Pandora's departmental structure (e.g. HR, Finance, IT). This structure allows for easy delegation of administrative tasks and user management.

Step 3: Enforce Password and Access Policies

Once AD is configured, establish strong password policies (e.g., minimum 12-character passwords, mandatory password expiration) and enable multi-factor authentication (MFA) where possible. Set up role-based access controls to ensure users can only access systems and data they need for their work.

Step 4: Implement Centralized Update Management

Deploy Windows Server Update Services (WSUS) or Microsoft Intune to centrally manage and push software updates to all computers. This ensures that all systems are kept up to date with the latest security patches.

Step 5: Standardize Security and Software Configurations

Use Group Policy to enforce security settings (e.g. firewall rules, antivirus settings, encryption standards) and standardize software installations across all systems. Group Policy also allows for automatic installation of required software and restrictions on non-authorized applications.

Step 6: Train Employees and Support Transition

Change management is crucial for the success of this transition. Organize training sessions for employees to introduce them to the new system, focusing on the importance of adhering to the new password policies and security practices. Create support documentation and ensure IT staff are readily available to assist employees with the transition.

Step 7: Monitor and Adjust

After the system is implemented, continuously monitor it using centralized tools like Microsoft Defender for Endpoint to detect any anomalies or security incidents. Adjust policies as necessary based on ongoing performance reviews and security needs.

5. Conclusion

The transition to a centralized user and system management system is critical for Pandora Company Limited to improve its security posture and operational efficiency. By implementing **Microsoft Active Directory** alongside centralized update management tools, Pandora will mitigate the risks associated with its current decentralized approach. Additionally, centralized management will streamline IT operations, improve employee productivity, and better protect sensitive company data.

6. References

- Control.com < https://control.com/technical-articles/cybersecurity-in-centralized-vs-decentralized-computing/ >
- Decryptouniversity.com < https://www.decryptouniversity.com/blog/centralized-vs-decentralized/ >
- Active Directory Pro < https://activedirectorypro.com/what-is-active-directory/ >

  < https://activedirectorypro.com/group-policy-best-practices/ >
- MS Active Directory < https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview/ >
- WSUS < https://learn.microsoft.com/en-us/windows-server/administration/windows-server-update-services/get-started/windows-server-update-services-wsus >
- Youtube links < https://www.youtube.com/watch?v=LOG-ewxwCOU/ >

  < https://www.youtube.com/watch?v=LkeGluvR6C8/ >