XEOX

ESSENTIAL IT SECURITY PRACTICES

for Modern Infrastructure

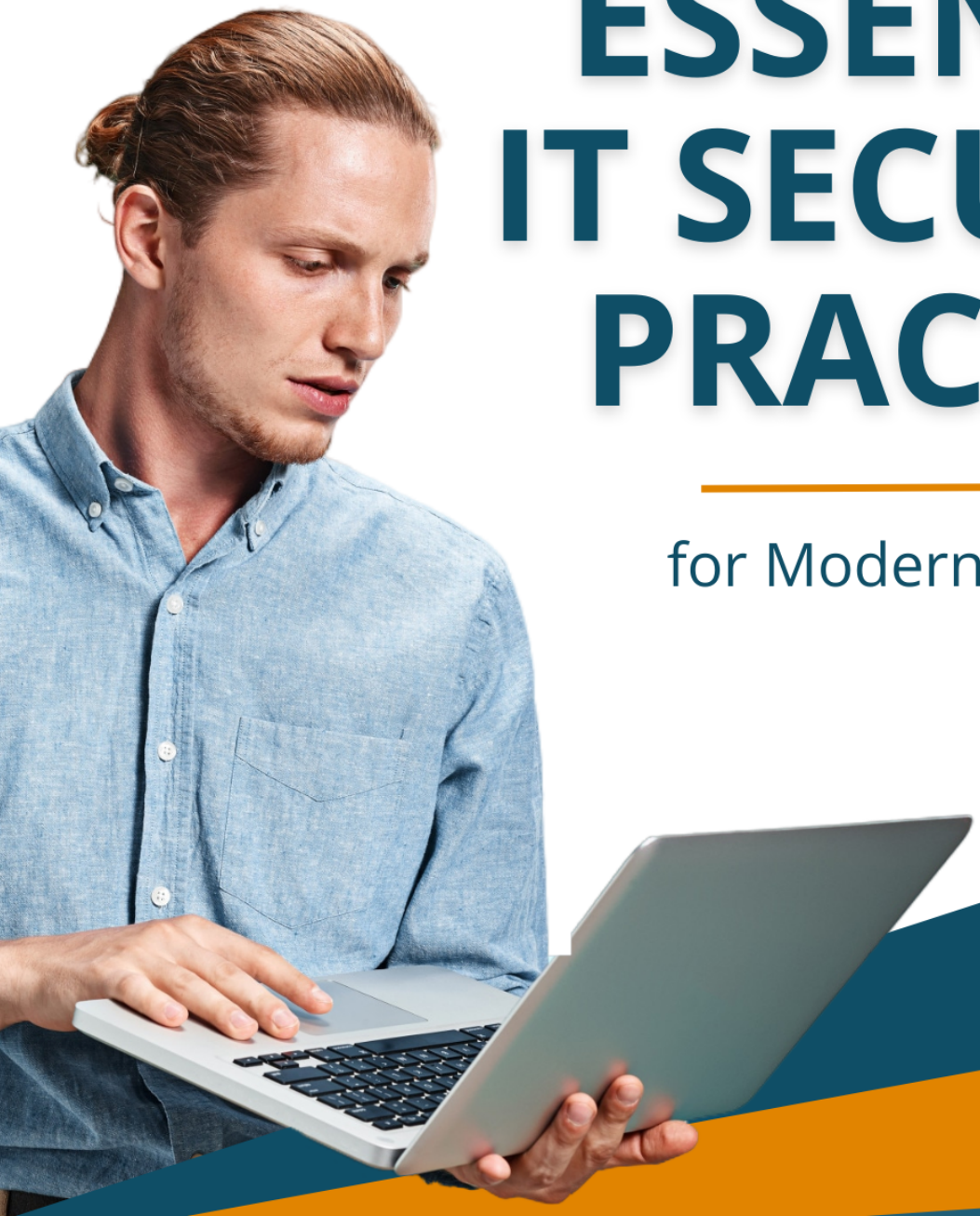

Table of Contents

Introduction	03
Admins Best Practices	03
Setup VLAN with ACL	04
Install Microsoft LAPS and Setup Policies	06
Procedure for isolating possibly Hacked Computers	06
Additional Backup Scenarios	07
Using Next-gen Antivirus	08
Remove/Verify Remote Access Tools	08
Domain Password Policy	09
Enable Windows Firewall	10
Install Cloud-Based RMM Tool	11
Internet Access on Servers	11
Client VPN	12
Citrix/ Terminal Server	12

Office 365 Security 13

Azure AD Premium and Risky User Report 14

Setup Monitoring Systems 15

Monitor AD Events 17

Firewall Best Practices 18

Legacy Device Management 19

Telephony and Production Systems 20

Databases / Backend Servers 21

INTRODUCTION

The rapid evolution of technology necessitates increasingly robust IT security measures to protect data and infrastructure. This eBook outlines best practices for maintaining a secure IT environment, focusing on essential aspects such as admin usage policies, VLAN setup, backup strategies, antivirus choices, and more.

ADMINS BEST PRACTICES

Effective management of administrative privileges is a cornerstone of IT security. By implementing strict usage policies and utilizing dedicated administrative tools, organizations can significantly reduce the risk of unauthorized access and potential system breaches. This section delves into the essential practices that every IT admin should follow to maintain a secure operational environment.

Admins Only Use Personal Account for Daily Work

Admins should always use personal accounts for daily tasks, ensuring these accounts do not have administrative rights. This strategy

reduces the risk of accidental changes and compromises if the account is exposed. Personal accounts should perform regular tasks, while admin accounts should be reserved strictly for activities that require elevated privileges.

Use Admin JUMP Server

Utilize an Admin JUMP server for all administrative operations. This is a dedicated server where administrators log in to perform tasks requiring elevated permissions. It centralizes administrative activities, allowing for better monitoring and auditing, reducing the attack surface by limiting where admin credentials are used.

Hyper-V and vCenter Login Policies

Hyper-V servers should either not be part of the main domain or placed in a separate, dedicated domain. This separation prevents potential cross- domain security breaches.

For vCenter, logins should be restricted to local accounts or a dedicated domain. This means domain accounts with broader access should not be used to log in to vCenter, enhancing security by limiting potential attack vectors.

SETUP VLAN WITH ACL

Segmenting network traffic using VLANs (Virtual Local Area Networks) with ACLs (Access Control Lists) improves security by isolating sensitive areas of your network and enforcing individual access policies.

MGMT VLAN

This VLAN should host management interfaces like Integrated Lights-Out (ILO), Dell Remote Access Controller (DRAC), VM Hosts, and vCenters. Ensuring management interfaces are in their VLAN helps protect them from being accessible by unauthorized users and limits exposure to threats.

Server VLAN

Contains user-facing servers such as application servers, web servers, and file servers. This VLAN should be closely monitored, and ACLs should be configured to restrict unnecessary access from outside this VLAN.

Backend Server VLAN

Host backend servers like SQL servers and other databases, which are typically not directly accessed by end users. This VLAN is isolated to improve security and performance

Admin VLAN

Devices within this VLAN are primarily used for administrative purposes and should have access to secured servers as needed. Limiting this VLAN to admin devices ensures that regular user activities do not interfere with administrative tasks or expose critical points to attackers.

INSTALL MICROSOFT LAPS AND SETUP POLICIES

Microsoft Local Administrator Password Solution (LAPS) allows secure management of the local administrator passwords for domain-joined computers, ensuring these passwords are frequently updated and securely stored in Active Directory. This reduces the risk of lateral movement within the network.

Define LAPS Policies: Ensure password complexity and change frequency are in line with company security policies.

Deploy LAPS: Ensure all domain-joined computers are configured to use LAPS.

PROCEDURE FOR ISOLATING POSSIBLY HACKED COMPUTERS

When a computer is suspected to be compromised:

Isolate from Network

Disconnect the device immediately from the network to prevent the spread of malware or unauthorized access.

Login with Local User or Local Admin

Investigate using local user or admin accounts only, preferably those managed via LAPS, to ensure the compromised device does not reconnect with domain credentials that could be further exploited.

ADDITIONAL BACKUP SCENARIOS

Develop backup strategies that are separated from the domain network to ensure resilience against breaches and ransomware.

Offsite and/or Offline Backups

Ensure data redundancy by maintaining offsite or offline backups, which can be crucial for disaster recovery.

1. Offsite Backups: Store backups in a geographically separate location.

2. Offline Backups: Keep backups on storage devices that are not continuously connected to the network to protect against network-based attacks.

USING NEXT-GEN ANTIVIRUS

Advanced antivirus solutions like Crowdstrike or Fireeye provide enhanced security features beyond traditional antivirus software, including:

Threat Detection and Response: Capabilities to detect and respond to advanced threats.

Behavioral Analytics: Analyze patterns to detect suspicious activity.

REMOVE/VERIFY REMOTE ACCESS TOOLS

Remote access tools, while necessary for certain operations, can pose significant security risks if not managed properly. This section provides guidance on how to minimize these risks by reducing permanent remote access points and implementing secure, on-demand solutions that restrict access to only when it's needed.

Reduce Permanent Remote Access

Eliminate unnecessary persistent remote access tools (e.g., Teamviewer Hosts), as these can be exploited by cyber attackers.

Secure On-demand Solutions

Opt for secure, on-demand remote access solutions that eliminate the need for always-on agents. This reduces the attack surface and ensures access is only granted when necessary.

DOMAIN PASSWORD POLICY

A robust domain password policy is a fundamental aspect of securing your IT environment. This section emphasizes the importance of regular password updates, the minimization of domain admin accounts, and the enforcement of strong, complex passwords across the organization to prevent unauthorized access.

User Password Changes

Implement policies requiring users to regularly change their passwords, particularly after account activation. Frequency should be balanced to ensure security without causing user frustration.

Change Service and Admin Passwords

Regularly update service account and domain admin passwords to minimize risks associated with outdated or compromised credentials.

Minimize Domain Admins

Keep the number of domain admin accounts to a minimum and limit their usage strictly to domain controllers, reducing the risk of administrative misuse.

ENABLE WINDOWS FIREWALL

Activating Windows Firewall on all clients and servers is essential for protection. If configuring the firewall directly on Windows systems proves challenging, leverage VLAN-based ACLs.

Allow Admin JUMP Hosts

Restrict administrative accesses like RDP, SSH, and remote management exclusively to Admin JUMP Hosts, with exceptions carefully managed for file and print servers.

INSTALL CLOUD-BASED RMM TOOL

A cloud-based Remote Monitoring and Management (RMM) tool such as Xeox ensures effective monitoring and regular updates for both clients and servers, particularly beneficial for remote and home office devices.

Client Management

- Upgrade to Supported Windows Versions: Maintain system integrity by ensuring all clients are running supported versions of Windows.
- Regular Updates: Utilize policies or RMM tools to ensure systems receive timely updates.

Server Management

Automate Patching: Implement automated patching processes using CRON jobs to ensure servers are up to date with the latest security and functionality patches.

Find out more about XEOX: https://xeox.com

INTERNET ACCESS ON SERVERS

Limiting server internet access to only essential sites is a critical security measure. This section advocates for a whitelist approach, ensuring that servers can only access pre-approved sites, thereby minimizing the risk of exposure to malicious content and potential attacks.

Whitelist Approach

Adopt a whitelist model for server internet access, allowing only pre-approved sites necessary for updates and operations.

CLIENT VPN

Eliminate Client VPNs if possible due to their security risks. If indispensably required:

- Enforce ACLs and 2FA: To secure VPN connections and minimize potential threats.

CITRIX / TERMINAL SERVER

Transitioning from traditional client VPNs to Citrix or Terminal Server environments can enhance security by centralizing access control.

This section covers the steps necessary to secure these gateways, including regular updates and the implementation of multi-factor authentication to protect against unauthorized access.

Migrate from Client VPN

Transition from Client VPNs to Citrix or Terminal Server scenarios, enhancing security and centralizing access control.

Update and Secure Gateways

Ensure Netscaler/TS gateways are always updated to the latest version and that 2FA solutions are in place.

OFFICE 365 SECURITY

Office 365 is a critical component of many organizations' IT infrastructure, making its security paramount. This section provides a comprehensive overview of the security measures available within Office 365, including two-factor authentication, conditional access policies, and data loss prevention strategies, to protect your organization's sensitive data.

Enable 2FA (Two-Factor Authentication

Activate two-factor authentication (2FA) for all Office 365 accounts to add an extra layer of security. 2FA requires users to provide a second form of verification, such as a code from a mobile app, in addition to their password, which significantly reduces the risk of unauthorized access even if passwords are compromised.

Conditional Access Policies

Implement conditional access policies within Office 365 to enforce rules based on user location, device type, or risk level. For example, you can block access from unfamiliar locations or require MFA for sign-ins from new devices,

thereby strengthening your security posture.

Data Loss Prevention (DLP) Policies

Set up Data Loss Prevention (DLP) policies to prevent sensitive information from being shared inappropriately. DLP policies can automatically identify and block sensitive data like credit card numbers, social security numbers, and other personally identifiable information (PII) from being emailed or shared externally.

Email Security Enhancements

Utilize Office 365's built-in features like Advanced Threat Protection (ATP) to safeguard against phishing, malware, and ransomware attacks. ATP includes capabilities such as Safe Links and Safe Attachments that proactively protect users from malicious content.

Regular Security Audits

Conduct regular security audits of your Office 365 environment, reviewing user permissions, access logs, and security settings. Audits can identify potential vulnerabilities or misconfigurations that might be exploited by attackers.

AZURE AD PREMIUM AND RISKY USER REPORTS

Acquire Azure AD Premium Licenses

Azure AD Premium provides advanced security features that are essential for protecting your organization's identity and access management. These features

include conditional access, identity protection, and Privileged Identity Management (PIM), which help safeguard against identity theft and unauthorized access.

Risky User Detection and Reporting

Utilize Azure AD Premium's Identity Protection to monitor for risky sign-ins and potentially compromised user accounts. Risky user reports leverage machine learning to analyze sign-in behavior and flag anomalies such as unusual locations, unfamiliar devices, or atypical access patterns.
Early detection allows for proactive measures like enforcing MFA, blocking access, or initiating password resets to mitigate risks.

Implement Just-in-Time Access with PIM

Privileged Identity Management (PIM) within Azure AD Premium enables just-in-time (JIT) access for administrators, reducing the risk of persistent privileged access. Admins can elevate their permissions only when necessary, and the access is time-bound, ensuring that elevated permissions are automatically revoked after a set period.

Automated Responses to Risky Sign-Ins

Configure automated responses to risky sign-ins, such as requiring MFA, blocking access, or notifying administrators. These automated actions help to swiftly contain potential security incidents and prevent unauthorized access from escalating.

SETUP MONITORING SYSTEMS

Continuous monitoring is key to maintaining a secure and resilient IT environment. This section discusses the deployment of comprehensive monitoring tools, log aggregation techniques, and the integration of automated incident response protocols to ensure that potential issues are detected and addressed promptly.

Deploy Comprehensive Monitoring Tools

Implement monitoring systems like Checkmk, Nagios, or Zabbix to continuously oversee infrastructure components, network traffic, and security events. These

tools can monitor servers, applications, network devices, and even cloud services, providing real-time alerts for any anomalies or issues that require immediate attention.

Log Aggregation and Analysis

Use centralized log aggregation tools like Splunk, Graylog, or the ELK Stack (Elasticsearch, Logstash, Kibana) to collect and analyze logs from various sources across the IT environment.

Aggregating logs in a central location allows for comprehensive analysis, making it easier to detect patterns or anomalies indicative of a security breach or system failure.

Automated Incident Response

Set up automated incident response protocols using your monitoring systems. For example, when a critical alert is triggered, the system can automatically initiate predefined actions such as isolating affected systems, alerting IT personnel, or even rolling back to a known good configuration.

Regular Health Checks and Performance Monitoring

Conduct regular health checks and performance monitoring to ensure all systems are functioning optimally. This proactive approach helps identify and resolve potential issues before they can impact business operations or be exploited by attackers.

Integration with SIEM Solutions

Integrate your monitoring systems with a Security Information and Event Management (SIEM) solution to enhance threat detection and incident response. SIEM solutions like IBM QRadar, ArcSight, or Microsoft Sentinel can correlate data from multiple sources, providing a comprehensive view of your security posture and enabling faster detection of sophisticated attacks.

MONITOR AD EVENTS

Active Directory (AD) is a critical component of IT infrastructure, making it essential to monitor AD events for any signs of unauthorized access or changes. This section outlines best practices for configuring audit policies, setting up automated alerts, and regularly reviewing AD logs to maintain the integrity and security of your directory services.

Comprehensive AD Event Monitoring

Implement continuous monitoring of Active Directory (AD) events to detect unauthorized access, changes to critical configurations, or unusual login activity. Monitoring tools should be configured to track a wide range of events, including user account changes, group membership modifications, and login failures, which could indicate a potential security incident.

Audit Policy Configuration

Ensure that AD audit policies are configured to log critical events such as successful and failed login attempts, changes to security policies, and modifications to user privileges. These logs are invaluable for investigating security incidents and ensuring compliance with regulatory requirements.

Automated Alerts for Suspicious Activity

Set up automated alerts for suspicious activities, such as an unusually high number of login attempts, changes to privileged accounts, or the creation of new admin accounts. These alerts enable rapid response to potential security threats, allowing IT teams to investigate and mitigate risks before they escalate.

Periodic Review of AD Logs

Regularly review AD logs to ensure no unauthorized changes or suspicious activities go unnoticed. Establish a routine where logs are analyzed for any patterns that might suggest security weaknesses, such as repeated login failures from specific IP addresses or unexpected modifications to group policies.

Backup and Recovery of AD

Ensure that your Active Directory is regularly backed up, and you have a robust recovery plan in place. In the event of a compromise, being able to quickly restore AD from a clean backup can prevent extended downtime and limit the impact of the attack.

FIREWALL BEST PRACTICES

Firewalls are a fundamental line of defense in network security. This section discusses the best practices for configuring firewalls, including the use of Static NATs, SSL inspection, and the activation of advanced firewall features to enhance security and visibility within your network.

Static NATs and DMZ

Regularly audit and verify NAT settings, moving necessary devices to a DMZ and segregating them by service.

SSL Inspection

Enable SSL inspection for both client and server communications using self-signed certificates if necessary, to intercept and analyze encrypted traffic.

Next-gen Firewall Blades

Activate advanced firewall features to provide enhanced security and visibility.

LEGACY DEVICE MANAGEMENT

Legacy devices often present security challenges due to outdated software and hardware limitations. This section provides guidance on how to effectively manage these devices, including isolation strategies and strict access controls, to minimize their potential risk to the broader network.

Isolate Legacy Devices

Legacy devices that cannot be updated or secured effectively should be isolated from the rest of the network using VLANs or dedicated firewall rules. These devices should be closely monitored for unusual activity.

Implement Access Controls

Use strict access controls and monitoring for legacy systems, and plan for their replacement or upgrade as soon as possible.

TELEPHONY AND PRODUCTION SYSTEMS

Telephony and production systems are critical components of business operations that require robust security measures. This section covers the best practices for securing VoIP systems and ensuring that production systems are protected from unauthorized access and monitored for any suspicious activity.

Secure VoIP Systems

Ensure that VoIP (Voice over IP) systems are secured with encryption and access controls to prevent eavesdropping or unauthorized use.

Protect Production Systems

Production systems should have restricted access, with multi-factor authentication (MFA) and strict monitoring of all changes or access attempts.

DATABASES / BACKEND SERVERS

Databases and backend servers store some of the most sensitive information within an organization. This section emphasizes the importance of encrypting data, performing regular backups and audits, and implementing strict access controls to protect these critical assets from unauthorized access and breaches.

Database Encryption

Encrypt sensitive data within databases to protect it from unauthorized access. This includes both data at rest and in transit.

Regular Backups and Audits

Perform regular backups and audits of backend servers to ensure data integrity and quick recovery in case of a breach.

Access Control

Limit access to backend servers and databases strictly to authorized personnel, using role-based access controls (RBAC) to enforce permissions.

Streamline your IT Management with Ease

find out more about our RMM- Tool
https://xeox.com

Need help?

Contact us:
Phone: +43-720-505765
E-Mail: support@xeox.com

Learn more about related Topics
https://xeox.com/blog

XEOX