OLD DOMINION UNIVERSITY

Network Infrastructure Project

IT417: Management of Information Security

Jacquez Pierre
Gerkeil Owens
Austin Black

11/13/24

Table of Contents

Introduction

Mission Statement:

The objective of this project is to apply our take on how the Strome College of Business's network should be built and apply various policies of security to ensure that the network is protected from bad actors, malware, or incidents.

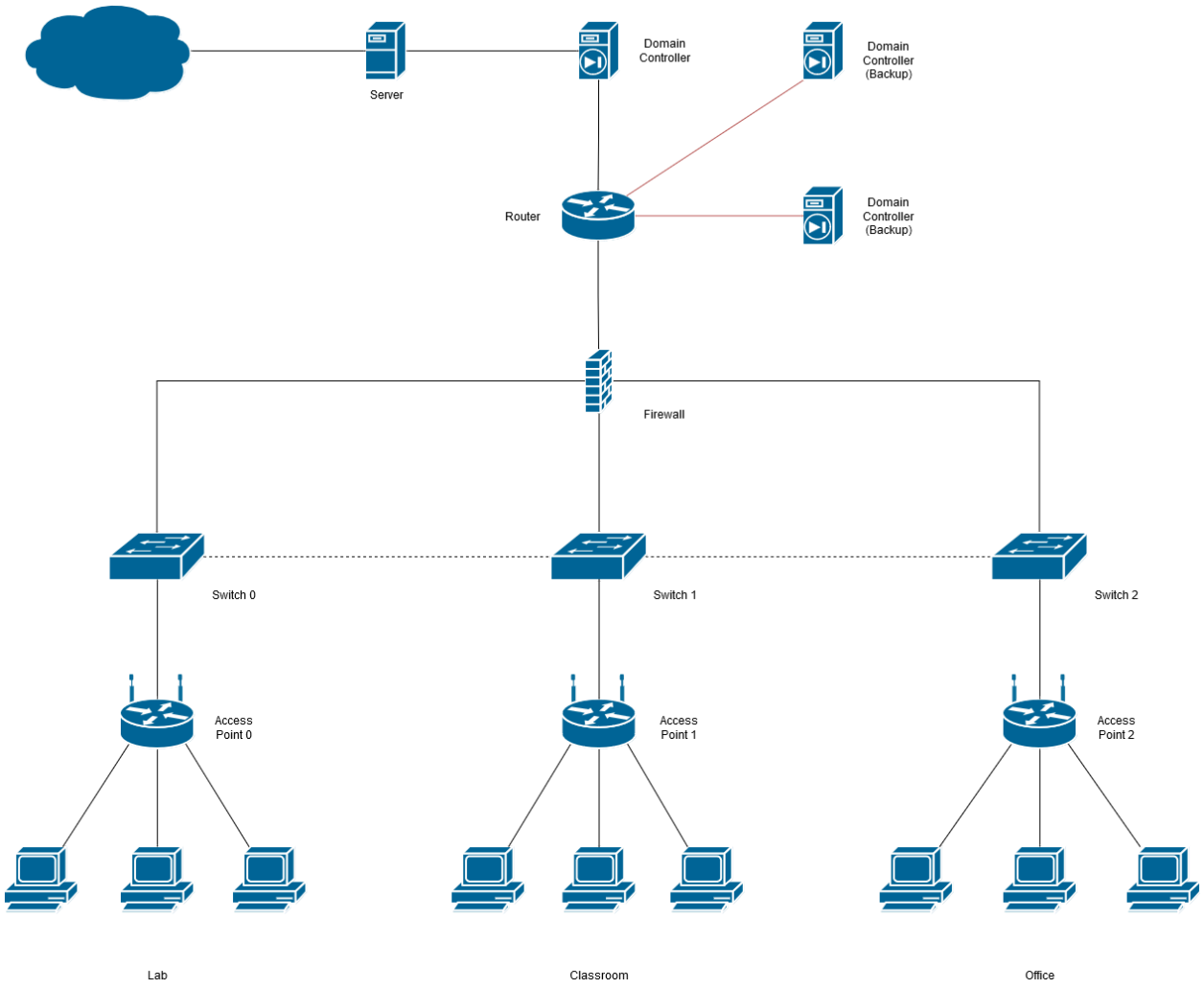
Opening:

In this document, we are establishing a good fundamental networking structure that will be beneficial for all the overall subnet within the Strome College of Business. What will be provided are an in depth view of network security for each required subnet. This is completely based on interpretation of what we believe will be great. This includes an overall specifications sheet, various diagrams regarding networking structure, implementation of security policies, and a breakdown on all of our findings during the research process of this assignment. The items that will be provided includes but not limited to 200 computers, domain controllers, NAS, and servers. The table below will provide the specifications of our project.

Specifications List:

1) Computers: Windows
    a) XPS Desktop ($549.99)
    b) Optiplex ($669)
    c) Optiplex All-In-One ($1,109)
2) Router: Cisco ISR 931 ($1,229.06)
3) Switches: Cisco Catalyst 2960 series ($1,795)
4) Server: Dell PowerEdge ($ 1,179)
5) Access Point: Cisco Meraki ($1,245)
6) Firewall: Fortinet ForGate ($695)
7) Domain Controllers: Microsoft AzureAD (monthly fee: $0.06)
8) Backup Solution: Veeam Backup & Replication ($1,710 per year)

Network Map


Server
Domain Controller
Domain Controller (Backup)
Router
Domain Controller (Backup)
Firewall
Switch 0
Switch 1
Switch 2
Access Point 0
Access Point 1
Access Point 2
Lab
Classroom
Office

Section 1: The Network

Mapping out the network

To get started building the network, the building was mapped out in detail and subnets were depicted for the overall network. The decided subnets were the computer labs, the classrooms, and the faculty offices. To ensure a secure connection will be available. Throughout research was performed on what kinds of tools should be used and where they should be placed and between all the subnets, it is believed that the computer lab will be the most crucial as it will hold an area for the server and other important components. Within one of the computer labs there will be the building's main files server. The reason is so students may access these servers as a part of their studies and faculty can easily access it.

File/Web Server

Dell's PowerEdge R260 was the selected server to handle files and applications within a sandbox environment. The file server will be running windows server 2022 as it is the most used server operating system. For the directory structure of the server, files are configured in a hierarchical structure. Premissions on the server will be set by different groups. These groups include students, faculty, and administrators. Administrators will have total control over the whole server to ensure the server's health and security. Administrators job is to not only provide for the servers but also ensure the safety of the students and faculty alike that are using it.

Faculty and Students will have limited access to the server where their premission only aligns with what they are allowed to access. It should be noted that Faculty will have more permissions than students as instructors and office personnel need specialized access to manage sensitive information concerning students, lesson plans, grades, or anything else that is needed. Students will only be limited to what their lesson plans consist of. For example, needing access to a sandbox environment for cyber security practices. Backups have also been planned during the events of losing critical information or if the whole server itself goes down. The chosen solution for this moment was to use Veeam Backup & Replication.

Domain Controllers

Domain controllers are responsible for the management of the network and identify security requests (Solarwinds, 2024). They act as gatekeepers for the network, validating users' privileges to indicate if they have authorization to access a specific resource within the network's domain. The validation process includes group policies, user credentials, and computer names. For this network, the domain controller that is being used is Microsoft Azure AD. Microsoft Azure AD is a cloud-based model that can be used to set up a domain controller for Windows Server 2022.

With this services faculties are able to not only monitor networking activities but also manage the active directory. To configure the domain controllers we must set up organizational units (OU) to handle organizing users, computers, and any other elements required within the network. Ensure group policies to provide security, installing software, and configuring changes within the group. Separate domain controllers will be used for the practice of redundancy. This way if something were to happen to the domain controller another one will be ready to take its place as maintenance is performed on the downed one. This will help eliminate any setbacks that may occur within the network. It's also important to ensure that backups are up-to-date so restoration can be as close as possible to current materials.

Router

The router is a core component for this network and essential for other devices to be able to perform their job. In this network the router that is being used is the Cisco ISR 931. This router will be beneficial to the network because it is built to make network management easier. Cisco 900 series routers have built in WAN, Switching if needed, security, and advanced connectivity features. This router will be the provided VLAN interface that will allow routing between three subnets giving each their own IP addresses. On the configuration side, the router will enable inter-VLAN so the three subnets can communicate with each other. An access control list will also be implemented so that network traffic can be moderated.

With the access control list it will be possible to block students from gaining access to resources that are exclusively available to the faculty. Configuring the quality of service (QoS) will help the router prioritize traffic that is coming from the file server and domain controllers. This will ensure proper performance for users within the network. Using the built-in switches within the router, the domain controllers should be able to connect to the router and be assigned the appropriate IP addresses. This is also important for the connectivity of both the file and web server.

Firewall

This is another crucial step for the network as the firewall provides the security for the whole infrastructure. The firewall that is being used within this network is the Fortinet ForGate 60F. The ForGate 60F is a NGFW with 1 Gbps, 700 Mbps of thread protection, 1.4 Gbps of IPS, and multiple GE RJ45 interfaces. To implement this into the network, configuring the firewall rules and pointing out the demilitarized zone (DMZ) must be done. In terms of setting up the firewall rules the VLAN will be isolated to ensure students will not be able to access faculty resources that contain critical information. Internal communication between devices that are within the internal zone will be permitted for users to gain access to domain authentication and file sharing.

For the DMZ, limited controlled access to resources will be implemented. The critical part for this configuration is to ensure that web servers within the DMZ are able to communicate to the internal servers, however exposure must be kept at a minimum. Outbound access will be enabled to allow both students and faculty to use the internet, however certain traffic will be restricted. Web filtering and malware protection must be prioritized at all times. Inbound access on the contrary will be restricted to certain services.

Switches

Upon completion of the firewall it is time to set up the switch for the network. In this network the switch that is being used is the Cisco Catalyst 2960 series. The switches will be connected to the firewall which is connected to the router. Each subnet has their own switch and all of them are configured to create a VLAN network. Upon

creating the VLAN on each switch it is time to configure the ports to ensure each switch will be able to read the traffic within the network between each other.

A management VLAN can also play a role as a method to create smaller networks within the network. The switch's interface can be more manageable; this benefit can improve the security of the overall network. Another advantage is that it can help with traffic flow which will prevent broadcast storms from occurring.

Access Point:

Access points should be more simple to configure compared to all the other components of the network. The access point that is being used in this network is the Cisco Meraki. Cisco Meraki utilizes WI-FI 6/6E so both students and faculty can take advantage of the strong connection. The access point also provides adaptive security, meaning this access point will have the ability to self configure and self maintain itself over the network. So all users and administrators can have a peace of mind while maintaining the network. What needs to be done is get each of the access points from each subnet connected to their switches and then configure the VLAN of them.

The Lab, The Classroom, and The Office

With the full network out on display along with planned mapping of the network on figure 1. Now it's a good time to discuss each subnet on their own. Inside the computer lap it was estimated that up 50 to 100 computers can potentially be used in each lab room. The number of labs there are within the building are solely based on the building architecture. It is to remember that only one out of the multiple labs will contain a full server along with other networking components as others will simply have access points and computers. The computer within the lab will be Dell's XPS desktop computer. These computers can help students with their assignments while also allowing students to do any projects whether it is on the hardware or using a virtualized sandbox.

The classrooms are a little different, classrooms are believed to be not as big as the computer labs so the number of computers are focused between 25 to 30. In a more condensed space it is recommended that classrooms will use Dell Optiplex computers as their small size will not take up space allowing more desks room for students and faculty. Finally the office space should be the easiest setup as for things to account for is the loft areas, cubicle spaces, and individual rooms. With all of this to account for the Dell Optiplex All-In-One would be great for faculties as it is powerful enough for them to

set up assignments or handle any other workplace tasks.

Section 2: Threats and Vulnerabilities

1. Possible threats and attacks

With the design and infrastructure of the network at Strome College of Business, here are some of the possible threats and attacks that could affect the network.

- Malware(Viruses, Trojans , Ransomware)- Malware can be introduced through phishing emails, infected USB drives, or malicious websites. Once inside, it could spread across systems and compromise sensitive data.

- Denial of Service and Distributed Denial of Service attacks- Attackers could flood the web server or other critical services with excessive traffic, disrupting the availability of the website or internal services.

- Phishing and social engineering- Attackers could impersonate administrators to steal user credentials or gain unauthorized access to systems.

- SQL Injection and Web application attacks- If the web applications are improperly configured or coded, attackers could exploit vulnerabilities like SQL injection to access or manipulate sensitive data bases.

- Privilege escalation- An attacker might exploit vulnerabilities to gain high privileges, potentially compromising sensitive resources or entire systems.

- Man in the middle attacks- Without proper encryption, sensitive data could be intercepted between users and internal servers.

- Data exfiltration- Sensitive academic and administrative data might be exfiltrated by malicious insiders or external attackers exploiting a breach.

- Inside threats- Disgruntled employees, or careless students or faculty could potentially cause harm to the system, such as leaking confidential information or causing data loss.

- Unauthorized access- Weak passwords or misconfigured access controls might allow unauthorized users to gain access to critical internal systems, servers, or sensitive data.

2. **Planning, Organization, Risk analysis, and Policies**

Asset	Threat	Vulnerability	Impact	Risk Level	Existing control	Mitigation actions
Faculty Systems	Malware, Phishing, Ransomware	Unpatched software, Weak password policies	Loss of data, compromise of academic work	High	Antivirus,Windows defender, GPO policies for updates	Enforce strict password policies, multi-factor authentication, regular patching
Web Server Web server continued…	DDoS, SQL Injection	Unsecured code, lack of filtering	Website downtime, data breach	High	Web Application Firewall	Regular code reviews, SQL injection prevention, DDoS mitigation strategies
Domain Controllers	Privilege Escalation, Insider Threat	Misconfiguration , Weak authentication	Full system compromised	High	Active Directory security, restricted access	Limit admin privileges, enable least privilege, multi-factor

						authentication on DCs
Network Attached Storage	Data Exfiltration,Ransomware	Lack of encryption, Weak access control	Data leakage, loss of research data	High	Encryption, backups	Enforce backup policies, implement full disk encryption
Student Workstations	Phishing, Malware, Unauthorized Access	Lack of restrictions on software installs	Data breach, system infection	Medium	Antivirus, Group Policy Restrictions	Restrict software installations, enforce device-level security policies

Existing Controls

- Existing controls the network has some key existing controls, such as firewalls, antivirus software, Group policy, encryption, and backup systems. However, there are still areas that need improvement, especially around access control and patch management.

Risk level and Mitigation

- The risks related to data loss, malware, and privilege escalation are high. Mitigation strategies that should be implemented include more secure access controls, encryption, robust patching policies, and user awareness programs.

Policies

- Acceptable Use Policy- Defines acceptable and prohibited actions on the network and system access.
- Access Control Policy- Enforces least privilege access, defining who can access what resources.
- Incident Response Policy- Establishes protocols for detecting, responding to, and recovering from security incidents.

3. Measures for ensuring confidentiality and authenticity

Encryption

- AES-256 encryption should be used for all sensitive data stored on the network attached storage and backups.
- SSL/TLS encryption for web traffic to protect data in transit between clients and the web server.
- BitLocker encryption on faculty and student desktops to protect against data theft in case of a breach or attack.

Justification

- Encrypting sensitive data ensures that even if data is intercepted or accessed without authorization, it cannot be read or used.
- SSL/TLS protects confidentiality and authenticity between clients and servers, mitigating risks such as man in the middle attacks.
- Bitlocker provides physical security for devices, ensuring data is encrypted if stolen or an attack was to occur.

VPN

- A VPN should be used for faculty and staff to securely access internal systems from off-campus locations.
- Multi-factor authentication should be mandatory for VPN access to ensure both the user's identity and device integrity.

VPN Justification

- A VPN ensures that data transmitted between remote users and the internal network is encrypted, preventing eavesdropping and data interception.
- Multi-factor authentication provides an added layer of security to protect against stolen credentials.

4. **Access control policies and implementation**

Access control policies ensure that users have only the minimum necessary privileges to perform their tasks.

1. **Role Based Access Control**
   - Role-based access control- Roles such as student, faculty administrator, and guest will be defined within the active directory.
   - Permissions to resources are granted based on the user's role.
2. **Least Privilege Principle**
   - Faculty and students will be granted only the minimal permissions required to access for their duties.
3. **Multi-Factor Authentication**
   - For accessing sensitive systems, multi-factor authentication will be implemented to add an extra layer of security.

- Use microsoft authenticator, duo mobile, or a hardware token for multi-factor authentication.

4. **Access Control Lists**

   - Access control lists will be implemented on the Network attached storage and file servers to restrict access to sensitive files based on roles and individual user needs.

5. **Active Directory Group Policies**

   - Group Policy Objects will enforce security settings, such as restricting local admin access on student and classroom systems.

Justification

- These measures ensure that only authorized individuals have access to critical resources, reducing the risk of unauthorized access or data breach.

- Multi-factor authentication adds an additional layer of protection, especially for high-value resources like administrative systems or servers.

Section 3: Policies

Policies for Intrusion Detection Systems

1. Policy Development

a. **Objectives and Scope**: The goal of the ODU IDS systems is to detect both unauthorized internal and external intrusions on public and private ODU owned systems. These IDS systems will protect all systems and devices under the Strome College of Business.
b. **Roles and Responsibilities**: The responsibility for management and control of the IDS system falls under ODU IT administration and its support groups.

2. Detection Policies

a. **Defining Intrusions**: An intrusion is classified as when an unauthorized person gains access to a system or resource. It can also refer to a series of security events that make up a security incident.
b. **Thresholds and Alerts**: Thresholds for each type of intrusion will be classified by their severity by the ODU IT administration. Alerts will also be handled by the ODU IT administration and handled by roles that the IT staff have selected.

3. Response Policies

a. **Incident Response Procedures**: The Strome College of Business will follow the NIST incident response lifecycle of Preparation, Detection and Analysis, Containment, Eradication, Recovery, and Post Event Activity.
b. **Escalation Protocols**: Depending on the Severity of an event the public as well as other branches of the ODU campus IT department may be notified if a breach was to occur.

4. Maintenance Policies

a. **Regular Updates**: Ensure IDS signatures and models are updated regularly with the most current information available to the college as well as the public.
b. **Continuous Monitoring**: Implement ongoing monitoring and periodic reviews. These reviews will be done monthly by Strome College of Business and quarterly by the entire ODU campus IT teams.

5. Access Control Policies

a. **User Access Levels**: IDS access will be the sole responsibility of the Strome College of Business and overall, ODU IT administration. Students and staff will not have access to any IDS permissions.
b. **Authentication and Authorization**: Authentication and Authorization will be the sole responsibility of the Strome College of Business and overall, ODU IT administration.

6. Data Retention Policies

a. **Log Management**: Log management will follow ISO 27001:2022 international standard for the proper collection, storage and use of logs and log management.
b. **Data Privacy**: It is both the user’s and Administrator's responsibility to effectively control and protect the privacy of the end user. The Strome College of Business will not be held responsible for any information privacy violation if it is the fault of the user.

7. Training and Awareness Policies

a. **Staff Training**: Higher level ODU and Strome IT leadership will be responsible for the regular training of IT staff on how to understand and operate IDS use.

b. **Awareness Programs**: Programs for learning will be implemented by IT leadership to enhance the learning of both IT and student groups.

8. Compliance Policies

a. **Regulatory Compliance**: All IDS policies must be in compliance with both ISO/IEC regulations as well as local and federal legislation.
b. **Audit and Reporting**: Regular audits and reports on IDS performance should be conducted by the ODU IT staff monthly.

9. Integration Policies

a. **System Integration**: IDS systems should be integrated into other protection systems set up by the Strome College of Business IT department.
b. **Compatibility**: Ensure compatibility with existing Strome College of Business security infrastructure.

10. Incident Documentation Policies

a. **Incident Logging**: All detected intrusions and responses should be well documented and reported to the appropriate leadership positions.
b. **Post-Incident Analysis**: Conduct analysis to improve future responses.

II. Implementation of Intrusion Detection Systems

1. Planning and Preparation

a. **Assessing Needs**: The Strome College of Business should conduct a thorough assessment of organizational needs quarterly to understand the needs of both Admin, Faculty, and Students.
b. **Selecting Solutions**: IT staff should choose appropriate IDS solutions based on the assessment.

2. Deployment

a. **Network Architecture**: deployment of IDS should be planned based on the current and future network architecture of Strome College.

b. **Installation and Configuration**: Install IDS components and configure them according to policies, campus needs, and regulations.

3. **Testing and Validation**

a. **Initial Tests**: Conduct initial tests to verify functionality and effectiveness of all systems inside the Strome College.
b. **Fine-tuning**: Adjust detection rules and thresholds based on test results.

4. **Monitoring and Maintenance**

a. **Continuous Monitoring**: Implement continuous monitoring to detect and respond to threats in real-time.
b. **Regular Updates**: Ensure IDS signatures and detection models are regularly updated with currently known public and private signatures.

Host Hardening: Update Policies and Implementation

1. **Regular Patch Management**

a. **Policy Development**: The ODU IT leadership will create a formal patch management policy that outlines the frequency and process for applying updates.
b. **Patch Sources**: The IT administration must find trusted sources for obtaining patches and updates, such as official vendor websites.
c. **Patch Testing**: An implemented testing phase for patches must be done in a controlled environment before deployment to production systems. This will be conducted by the Strome IT staff.

2. **Automated Updates**

a. **Automation Tools**: Strome admin will utilize tools and software that automate the update process, ensuring timely application of patches.
b. **Scheduling**: Schedule updates during off-peak hours to minimize disruption to business operations. Peak hours include any afterschool, or weekend events that may be occurring inside Strome College.

3. **Critical and Security Updates**

a. **Prioritization**: Strome IT staff should prioritize critical and security updates to address vulnerabilities that could be exploited by attackers.
b. **Emergency Patching**: Strome IT staff should develop procedures for emergency patching in response to zero-day vulnerabilities or active threats.

4. Compliance and Reporting

a. **Compliance Checks**: Strome IT staff should Regularly check systems for compliance with updated policies.
b. **Reporting**: Strome IT staff should Maintain logs and reports of applied updates for auditing and compliance purposes.

III. Implementation of Update Policies

1. Assessment and Planning

a. **Inventory Management**: Management and storage of all systems and software including the update process will be handled by the appointed Strome IT personnel.
b. **Risk Assessment**: The Strome IT leaderships will conduct a risk assessment quarterly to identify critical systems and prioritize updates accordingly.

2. Deployment Strategies

a. **Staged Deployment**: Updates will be conducted in stages, starting with non-critical systems to identify potential issues before updating critical systems.
b. **Rollback Procedures**: IT Staff will establish rollback procedures to revert to previous versions in case of update failures or issues.

3. Monitoring and Verification

a. **Continuous Monitoring**: IT staff should monitor systems continuously to ensure updates are applied successfully and systems remain secure.
b. **Verification**: IT staff should verify the integrity and functionality of systems after updates are applied.

4. User Training and Awareness

a. **Training Programs**: Conduct training programs for IT staff and end-users on the importance of updates and how to recognize update-related issues.
b. **Awareness Campaigns**: Run awareness campaigns to keep users informed about the latest updates and security practices. This includes students, faculty, and public use.

IV. Additional Host Hardening Measures

1. Access Control

a. **Least Privilege**: The least privileged users are to be created by the Strome IT staff and should include students and publicly available computer access.
b. **Multi-Factor Authentication (MFA)**: MFA will be required of all personnel with an ODU registered account. This includes all faculty and staff of all departments. The currently used MFA for ODU is Duo.

2. System Configuration

a. **Disable Unnecessary Services**: The Strome IT. Administration should disable all services not needed per device group. As well as disabling services across the board that will not be used by any device inside of the Strome College to prevent unnecessary vulnerabilities.
b. **Secure Configurations**: Secure Configuration should abide by all Nist guidelines and follow the policies set by the Strome College of Business IT department and well as the overall ODU IT department.

3. Network Security

a. **Firewalls and Intrusion Detection Systems**: Storme will implement security features such as firewall and Intrusion detection systems to secure the privacy and authenticity of information under the college network.
b. **Segmentation**: IT staff will segment the network to isolate critical systems and limit the spread of potential attacks.

4. Regular Audits and Assessments

a. **Vulnerability Scanning**: It is the responsibility of the Strome IT department to conduct regular vulnerability scans to identify and address security weaknesses.
b. **Penetration Testing**: Strome IT administrators will conduct periodic penetration testing to evaluate the effectiveness of security measures and identify areas for improvement. This should be done quarterly to ensure the effectiveness of security measures.

Security for Software/Applications in a University Environment

1. **Software Installation Policies**

a. **Approval Process**: None IT administrators should submit a form to the Strome IT department for approval of any software not already approved by the Strome College of Business
b. **Authorized Software List**: The Strome College of Business will maintain a list of approved software that has been vetted for security risks. This list should be publicly found on Strome's website.
c. **User Permissions**: IT staff will restrict installation permissions to authorized personnel only, such as IT staff or faculty members.

2. **Access Control Policies**

a. **User Authentication**: Strome IT Administrators should Implement strong authentication mechanisms, such as multi-factor authentication (MFA), for accessing applications.
b. **Role-Based Access Control**: Administrators should assign access rights based on user roles to ensure users have only the necessary permissions.

3. **Data Protection Policies**

a. **Data Encryption**: All traffic moving both internally and externally through the Strome network should conform to the Advanced Encryption Standard. As well as the use of SSL and TLS techniques
b. **Data Retention**: Data retention should follow the standards and guidelines set by ISO 27001 to effectively protect and prevent the loss or leak of information.

4. **Update and Patch Management Policies**

a. **Regular Updates**: It is the responsibility of the Strome IT department to ensure that all software and hardware are regularly updated to the most secure and recent updates available.
b. **Automated Updates**: Automated tools will be implemented by the Strome IT staff to ensure updates are all done on time.

5. Incident Response Policies

a. **Incident Reporting**: The Strome users and IT staff should report any and all incidents to the IT department leadership for correct execution of any response needed.
b. **Response Plan**: Strome IT leadership will create a response plan to carry out any response to an incident that may happen inside and around the Strome College network.

III. Security Configurations

1. Application Hardening

a. **Default Settings**: Strome IT staff should change any and all default system settings to secure passwords to prevent unauthorized access to the network or systems.
b. **Disable Unnecessary Features**: IT staff will disable features and services that are not required to minimize the attack surface.

2. Web Application Security

a. **Input Validation**: Storme IT staff should Implement input validation to prevent common web vulnerabilities such as SQL injection and cross-site scripting (XSS).
b. **Secure Coding Practices**: All users should follow secure coding practices and guidelines to develop secure web applications for those who have access to it.
c. **Web Application Firewalls (WAF)**: the use of WAFs will be implemented by Strome IT Staff to protect web applications from malicious traffic.

3. Network Security

a. **Firewalls**: Strome IT staff will configure firewalls to control and monitor incoming and outgoing network traffic.
b. **Segmentation**: The Strome IT department will segment the network to isolate critical systems and applications from less secure areas.

4. Logging and Monitoring

a. **Activity Logs**: Strome IT Staff should create logs for any activities that occur on the network and properly store them based on policy guidelines
b. **Continuous Monitoring**: IT staff will implement continuous monitoring tools to identify and respond to security threats in real-time.

IV. Software Installation and Management

1. Who May Install Software

a. **IT Staff**: Primary responsibility for installing and managing software lies with the IT department.
b. **Faculty Members**: Faculty may be granted installation permissions for academic and research-related software, subject to approval.
c. **Students**: Generally restricted from installing software on university-owned devices, except in controlled environments such as computer labs.

2. Installation Procedures

a. **Security Review**: Strome IT leadership should conduct a security review of the software to identify potential risks and ensure compliance with university policies.
b. **Deployment**: Approved software is deployed using the standards and guidelines set by the Strome College of Business's IT department.

3. Software Inventory Management

a. **Inventory Tracking**: The Strome IT department should maintain an inventory of all installed software, including version numbers and licensing information.

b. **License Compliance**: IT is the responsibility of the Strome IT leadership to ensure that all software is compliant with the licenses granted to the college

Data Protection Measures

I. Policies

1. Data Classification Policy

a. **Classification Levels**: All data should be classified into different areas based on the importance of the information with different levels of security and access given to each level.
b. **Handling Procedures**: Each level of data should have its own procedure for handling and accessing the information.

2. Data Access Policy

a. **Access Controls**: IT leadership should implement role-based access controls (RBAC) to restrict access to sensitive data.
b. **Authentication**: all data access should require strong authentication methods, such as multi-factor authentication (MFA), for accessing sensitive data.

3. Data Retention Policy

a. **Retention Periods**: Data retention should follow the standards and guidelines set by ISO 27001 to effectively protect and prevent the loss or leak of information.
b. **Data Disposal**: Data disposal should follow the standards and guidelines set by ISO 27001 to effectively protect and prevent the information from being accessed by unauthorized parties

II. Technology

1. Encryption Tools

a. **Data at Rest**: Strom IT administrators should use encryption tools to protect data stored on servers, databases, and storage devices.
b. **Data in Transit**: IT administrators will implement encryption protocols such as TLS and SSL to secure data transmitted over networks.

2. Access Control Systems

a. **Identity and Access Management (IAM)**: The use of IAM systems is required to manage user identities and enforce access policies.
b. **Privileged Access Management (PAM)**:IT leadership will implement PAM solutions to control and monitor access by privileged users.

3. Data Loss Prevention (DLP)

a. **DLP Software**: The Strome College of business IT department should use DLP software to monitor and protect sensitive data from unauthorized access and exfiltration.
b. **Endpoint Protection**: the DLP software will require the use of endpoint protection tools to secure devices that access and store sensitive data.

4. Backup Solutions

a. **Automated Backups**: Strome IT administrators will implement automated backup solutions to ensure regular and consistent data backups.
b. **Encryption of Backups**: IT is the responsibility of the Strome IT department to ensure that backup data is encrypted to protect it from unauthorized access.

III. Backup Storage Locations

1. On-Premises Storage

a. **Local Servers**: Stored backups on local servers within the organization's data centers should be created with access to these backups only available to authorized personnel

2. Offsite Storage

a. **Remote Data Centers**: Store backups in remote data centers should be created to protect against local disasters.
b. **Physical Media**: Use physical media such as tapes, external hard drives will be stored in secure offsite locations.

3. Cloud Storage

a. **Cloud Backup Services**: The Strome IT department should utilize cloud backup services for scalable and cost-effective storage.
b. **Hybrid Solutions**: Combined on-premises and cloud storage for a hybrid backup strategy will be implemented by Strome to provide the best available protection for backups.

IV. Restoration/Recovery Measures

1. Backup Verification

a. **Regular Testing**: The Strome IT department should conduct regular tests to verify the integrity and recoverability of backup data.
b. **Checksum Validation**: IT administrators should use checksums to ensure data integrity during backup and restoration processes.

2. Recovery Procedures

a. **Disaster Recovery Plan**: It is the responsibility of the Strome IT leadership to create a disaster recovery plan for all storage locations and operations to insure the fastest possible recovery.
b. **Recovery Time Objectives (RTO)**: IT leadership will define the RTOs to ensure timely recovery of critical systems and data.
c. **Recovery Point Objectives (RPO)**: IT leadership establishes RPOs to determine the acceptable amount of data loss in the event of a disaster.

3. Documentation and Training

a. **Recovery Documentation**: All recovery operations should be well documented by both the active recovery team and leadership.
b. **Staff Training**: Leadership should conduct regular training sessions for IT staff on backup and recovery procedures.

Risk Assessment with Updated Controls and Cost-Benefit Analysis

I. Risk Assessment with Updated Controls

1. Identify Assets and Threats

a. **Assets**: Sensitive data, critical systems, intellectual property, user information.
b. **Threats**: Cyber attacks, data breaches, insider threats, system failures.

2. Evaluate Vulnerabilities

a. **Pre-Control Vulnerabilities**: Lack of encryption, outdated software, weak access controls.
b. **Post-Control Vulnerabilities**: Reduced due to implementation of encryption, regular updates, and strong access controls.

3. Assess Likelihood and Impact

a. **Likelihood**: This is the probability of an attack occurring both pre and post control.
    i. **Pre-Control**: High likelihood due to existing vulnerabilities.
    ii. **Post-Control**: Reduced likelihood due to mitigated vulnerabilities.
b. **Impact**: This is the potential amount of damage that may occur both pre and post control.
    i. **Pre-Control**: High impact due to exposure of sensitive data and critical systems.
    ii. **Post-Control**: Reduced impact due to enhanced protection measures.

4. Risk Level Determination

a. **Pre-Control Risk Level**: High risk due to high likelihood and impact.
b. **Post-Control Risk Level**: Moderate to low risk due to reduced likelihood and impact.

II. Cost-Benefit Analysis

1. Costs of Implementing Controls

a. **Initial Costs**: Initial costs of implementing controls include.
    i. Purchase and deployment of encryption tools, access control systems, and backup solutions.
    ii. Training programs for staff, administrators, and students.

b. **Ongoing Costs**: The costs that are reoccurring
    i. Regular updates and maintenance.
    ii. Continuous monitoring and compliance checks.

2. Benefits of Implementing Controls

a. **Risk Reduction**: The reduction in the amount of risk involved after implementing controls
    i. Significant reduction in the likelihood and impact of data breaches and cyber-attacks.

b. **Compliance**: The active following of the rules and policies set in place by the Strome College of Business
    i. Meeting regulatory requirements and avoiding legal penalties.

c. **Reputation**: The public's opinion on how they see Strome and its facilities.
    i. Enhanced trust and reputation among stakeholders and users.

d. **Operational Continuity**: The uptime on all the assets under the control of Storme.
    i. Reduced downtime and disruption due to improved recovery measures.

3. Quantitative Analysis

a. **Cost of Controls**: Overall cost of implementing and running added controls
    i. Initial investment: $4348.06
    ii. Annual maintenance: $1710.06

b. **Potential Losses Without Controls**: The estimated loss from not having controls

i. Estimated cost of a data breach: $100,000

ii. Estimated downtime cost: $5000 per incident

4. **Return on Investment (ROI)**

a. **ROI Calculation**:

i. Savings from avoided breaches and downtime: $160,000 Yearly

ii. ROI = 25.4x

Incident Response Plan

I. Incident Response Team

· **Roles and Responsibilities**: The roles and responsibilities should be clearly defined by the Strome IT department for key leadership positions such as the Incident Response Manager, IT Support, Legal Advisor, and Communication Officer.

· **Contact Information**: Contact information for all leadership positions and external parties should be regularly updated and maintained.

II. Incident Identification

· **Detection Methods**: The Strome IT department should use the combined efforts of IDS, SIEM systems, firewalls, logs, honeypots, and user reports to identify incidents.

· **Classification**: All incidents should be properly categorized and classified into different groups based on the severity and impact of the incident clarified by the Strome IT department.

III. Incident Response Procedures

· **Preparation**

  ○ Strome IT leadership should conduct regular training and simulations.

- The IT department should ensure tools and resources are ready and functioning correctly

· **Detection and Analysis**
  - The incident response team should verify the validity of the initial detection and ensure that there is a valid incident happening.
  - The incident response team should gather and analyze data to understand the scope of any and all incidents at hand.

· **Containment, Eradication, and Recovery**
  - Short-term: Strome's IT team is responsible for containment to prevent further damage.
  - Long-term: Strome's IT team should actively focus containment to isolate affected systems.
  - Strome's IT team should eradicate the root cause and recover systems to normal operation.

· **Post-Incident Activities**
  - All incidents should be documented post incident by both the incident response team and Strome IT leadership.
  - The entire Strome IT department as well as outside parties involved should conduct a post-incident review to identify lessons learned.

IV. Communication Plan

· **Internal Communication**: Strome IT Leadership will notify relevant stakeholders within the organization.

· **External Communication**: Strome IT Leadership will inform external parties such as students, community groups, legal teams, and regulatory bodies if necessary.

V. Continuous Improvement

· **Regular Updates**: IT leadership should review and update the incident response plan regularly.

· **Feedback Incorporation**: IT leadership should use feedback from incidents and drills to improve the plan. This includes forms regularly sent out to both students and staff on any issues they may have.

Disaster Recovery Plan

I. Disaster Recovery Team

- **Roles and Responsibilities**: It is the responsibility of the Strome IT leadership to create a disaster recovery plan for all storage locations and operations to insure the fastest possible recovery.

- **Contact Information**: Contact information for all leadership positions and external parties should be regularly updated and maintained.

II. Risk Assessment and Business Impact Analysis

- **Risk Identification**: Strome IT leadership should converse with Strome College leadership to identify potential risks and threats to the organization.

- **Impact Analysis**: Strome IT leadership should converse with Strome College leadership to identify and assess the impact of different types of disasters on business operations.

III. Disaster Recovery Strategies

- **Data Backup and Restoration**
    - The Strome IT department should regularly back up data and ensure backups are stored securely.
    - The Strome IT department should test data restoration procedures to ensure they work effectively.

- **System Recovery**
    - A plan for recovery procedures for critical systems and applications should be created by IT leadership.
    - It is the responsibility of IT leadership to ensure hardware and software requirements are documented.

- **Alternative Work Arrangements**
    - IT leadership should create a plan for remote work or temporary office locations if primary facilities are unavailable.

IV. Disaster Recovery Procedures

- **Activation**

- A criterion for when the activation of disaster recovery procedures should be created by IT and College leadership.
- The initial plans for recovery should be created and all IT personnel need to be informed of the outline.

- **Execution**
  - A detailed set of steps should be created by IT leadership on the steps that need to be taken by the Strome IT department when actively using DR procedures.
  - IT leadership should coordinate with external vendors, faculty and staff, and service providers on the next steps that will be taken after DR procedures have been implemented.

- **Testing and Validation**
  - IT leadership and the DR Team should regularly test the disaster recovery plan.
  - IT leadership and the DR Team should validate recovery procedures to ensure they are effective.

Bibliography

Dell. (n.d.). *Poweredge servers: Dell USA*. https://www.dell.com/en-us/shop/storage-servers-and-networking-for-business/sf/poweredge

What is a LAN (Local Area Network)? | cloudflare. (n.d.-d). https://www.cloudflare.com/learning/network-layer/what-is-a-lan/

Fortigate 900g series | data sheet. (n.d.-a). https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-900g-series.pdf

Cisco Catalyst 2960 Series switches. (n.d.). https://www.cisco.com/c/dam/global/de_at/assets/unified_partners/smb/vertriebliche-positionierung/switching/downloads/cat_2960_faq_e.pdf

Fortigate FortiWiFi 60F series data sheet. (n.d.-b). https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-fortiwifi-60f-series.pdf

Buckbee, M. (2023, June 16). *What is Azure Active Directory? A complete overview*. Varonis. https://www.varonis.com/blog/azure-active-directory

What is a domain controller? - it glossary. SolarWinds. (n.d.). https://www.solarwinds.com/resources/it-glossary/domain-controller

"Access Control Policies: Definitions & Types - Satori." *Satori Cyber*, https://satoricyber.com/access-control/access-control-policies-definitions-types/#types-of-access-control-policies. Accessed 2 December 2024.

Ayuya, Collins. "8 Different Types of Firewalls Explained (with Use Cases) | ENP." *Enterprise Networking Planet*, 12 April 2023, https://www.enterprisenetworkingplanet.com/security/types-of-firewalls/. Accessed 2 December 2024.

Cranford, JJ. "Incident Response Plan: Frameworks and Steps." *CrowdStrike.com*, 6 July 2023, https://www.crowdstrike.com/en-us/cybersecurity-101/incident-response/incident-response-steps/. Accessed 2 December 2024.

Ferraiolo, Chandramouli, and Ed Coyne. “Role Based Access Control | CSRC | CSRC.” *NIST Computer Security Resource Center*, 21 November 2016, https://csrc.nist.gov/projects/role-based-access-control. Accessed 2 December 2024.

“Group Policy Management Console in Windows.” *Microsoft Learn*, 22 April 2024, https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/group-policy/group-policy-management-console. Accessed 2 December 2024.

“How to Create a Cybersecurity Disaster Recovery Plan - Check Point Software.” *Check Point Software Technologies*, https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cybersecurity/how-to-create-a-cybersecurity-disaster-recovery-plan/. Accessed 2 December 2024.

Jain, Sandeep. “Advanced Encryption Standard (AES).” *GeeksforGeeks*, 16 July 2024, https://www.geeksforgeeks.org/advanced-encryption-standard-aes/. Accessed 2 December 2024.

“What Are Firewall Rules? | Firewall Rules Explained.” *Palo Alto Networks*, https://www.paloaltonetworks.com/cyberpedia/what-are-firewall-rules. Accessed 2 December 2024.

“What is the principle of least privilege?” *Cloudflare*, https://www.cloudflare.com/learning/access-management/principle-of-least-privilege/. Accessed 2 December 2024.

https://www.nist.gov/

https://itlaw.fandom.com/wiki/The_IT_Law_Wiki

https://www.fordham.edu/information-technology/it-security--assurance/it-policies-procedures-and-guidelines/

https://www.odu.edu/information-technology-services/computing-standards