Application Security (Written Assignment)

Full Name: Arshi Lamba

Admin No: 232619X

Tutorial Group: IT2163-02

I have chosen the following security features for my assignment:

1. Payment page with Credit Card info (Pg 2-9)
2. Data encryption archival

Statement on Plagiarism

I certify that this assignment/report is my own work, based on my personal study and/or research and that I have acknowledged all material and sources used in its preparation, whether they be books, articles, reports, lecture notes, and any other kind of document, electronic or personal communication. I also certify that this assignment/report has not previously been submitted for assessment in any other unit, and that I have not copied in part or whole or otherwise plagiarised the work of other students and/or persons.

| Signature |  |
| --- | --- |
| Date |  |

***Payment Page with Credit Card Info***

* *Security Issues*

1.1 Data Breaches

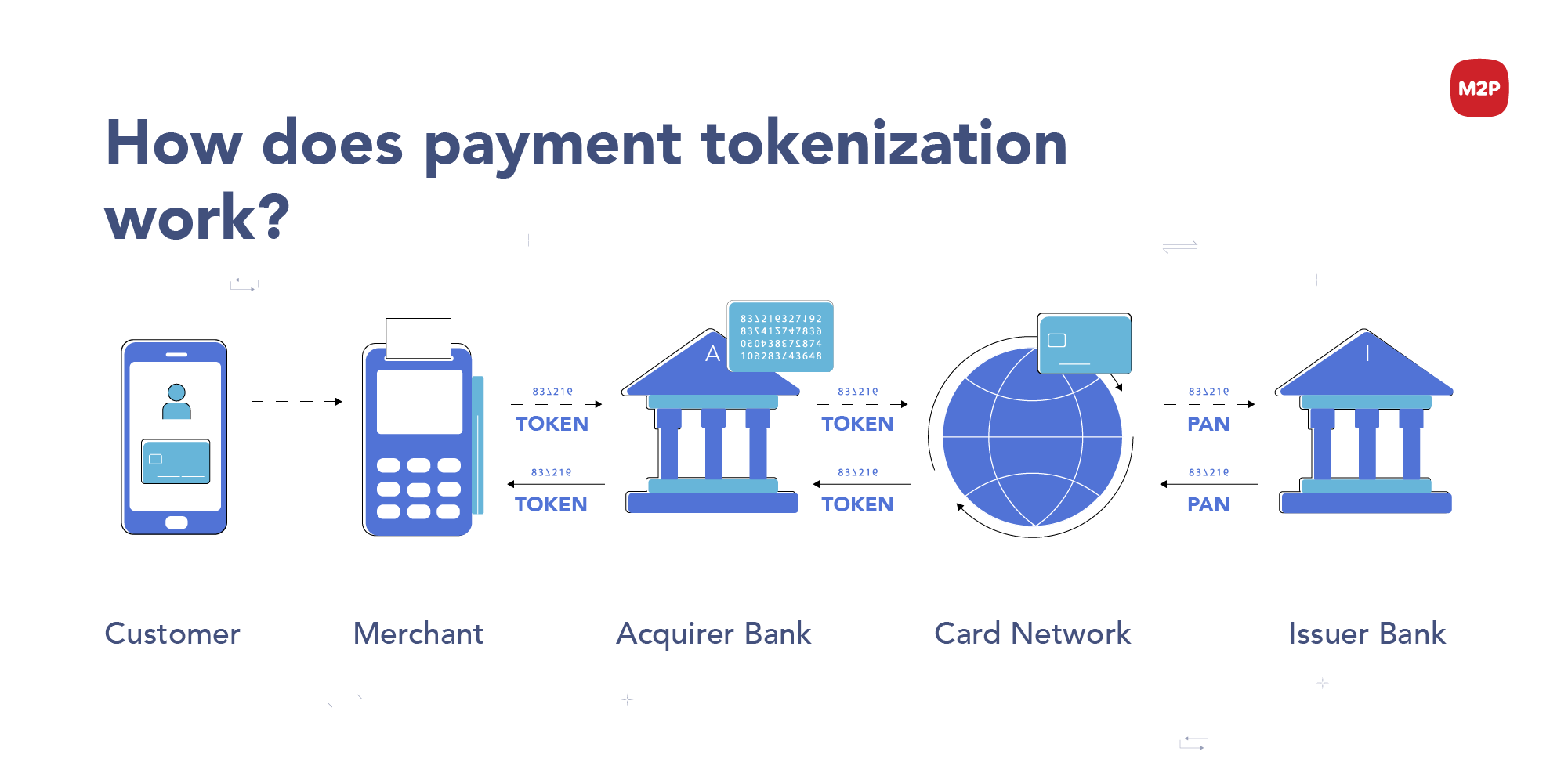
Description: A data breach is any security incident in which unauthorized parties access sensitive or confidential information, including personal data (Social Security numbers, bank account numbers, healthcare data) and corporate data (customer records, intellectual property, financial information).

Mitigation Techniques

* Tokenization

How is tokenization implemented in payment gateways?

1. Customers would initiate a transaction through an online checkout page. They would enter card details into the payment gateway on the website.
2. The merchant’s payment gateway then sends a request to the payment service provider, which tokenizes the customer’s credit card information.
3. The PCI-compliant payment service provider returns the token reference to the merchant and stores the token mapping to the payment credential data.
4. The merchant’s payment gateway may provision a network token for the card and use the network token - instead of the original card data - to request payment authorization from the card scheme and the customer’s bank.
5. After the issuing bank successfully authorizes the payment, they notify the merchant, and the payment is completed.



1. The merchant can then store the token for future transactions from that customer - be it for recurring payments, refunds, or to enable one-click payments - without failing foul of PCI DSS (Payment Card Industry Data Security Standard) compliance requirements.

Why is this solution effective in mitigating data breaches?

Tokens are unique identifiers that have no intrinsic value and cannot be used to recreate the original data. By tokenizing sensitive data, organizations can reduce the risk of data breaches and comply with data security regulations.

* Choose a PCI DSS Compliant Payment Gateway

Implementation:

There are 12 main requirements in the PCI DSS Security Standard which are supposed to be implemented:

1. Install and maintain network security controls
2. Apply secure configurations to all system components
3. Protect stored cardholder data
4. Protect cardholder data with strong cryptography during transmission over open, public networks
5. Protect all systems and networks from malicious software
6. Develop and maintain secure systems and software
7. Restrict physical access to cardholder data
8. Identify users and authenticate access to system components
9. Restrict physical access to cardholder data
10. Log and monitor all access to system components and cardholder data
11. Test security of systems and networks regularly
12. Support information security with organizational policies and procedures

Step-by-Step Procedure

1. **Know the requirements**

The first step in achieving PCI compliance is knowing which requirements apply to the organization. There are four different PCI compliance levels, typically based on the volume of credit card transactions the business processes during a 12-month period.

1. **Map data flows**

Before one can protect sensitive credit card data, one needs to know where it lives and how it gets there. One would want to create a comprehensive map of the systems, network connections, and applications that interact with credit card data across their organization. Depending on one’s role, one would probably need to work with your IT and security team(s) to do this.

First, identify every consumer-facing area of the business that involves payment transactions. For example, you may accept payments via an online shopping cart, in-store payment terminals, or orders placed over the phone.

Next, pinpoint the various ways cardholder data is handled throughout the business. It’s important to know exactly where the data is stored and who has access to it.

Then, identify the internal systems or underlying technologies that touch payment transactions. This includes one’s network systems, data centers, and cloud environments.

1. **Check security controls and protocols**

Once credit card data touchpoints are mapped across the organization, it is important for IT and security teams to implement the necessary security configurations and protocols, such as Transport Layer Security (TLS).

The 12 security requirements for PCI DSS are aligned with best practices for data protection, many of which also comply with privacy regulations like GDPR and HIPAA. Some of these requirements may already be in place within the organization.

1. **Monitor and maintain**

PCI compliance is an ongoing process that requires continuous attention, particularly as data flows and customer touchpoints evolve. Organizations may need to submit reports or complete assessments annually or quarterly, especially if processing more than 6 million transactions per year. Maintaining compliance typically involves collaboration across departments. A dedicated team should include security experts (CSO, CISO), technology/payment teams (CTO, VP of Payments), finance teams (CFO), and legal advisors to ensure compliance is properly managed.

Why is this solution effective in mitigating data breaches?

PCI compliance helps one prevent data breaches, PCI noncompliance fines, and lawsuits. By adhering to PCI DSS standards, businesses implement robust security measures that protect sensitive payment information, thereby minimizing the likelihood of data breaches.

1.2 Malware

Description: Malware describes malicious applications or code that damage or disrupts the normal use of endpoint devices. When a device becomes infected with malware, you may experience unauthorized access, compromised data, or being locked out of the device unless you pay a ransom.

Mitigation Techniques

* Patch Management

Implementation:

1. Inventory all IT assets: Identify and classify systems handling payment data
2. Categorize assets: Rank assets based on their importance to payment operations and risk exposure
3. Patch management requirements: Follow standards like PCI DSS, NIST 800-53, and SOC 2 for compliance.
4. Policy creation: Develop a patch management policy outlining roles, schedules, and procedures
5. Regular monitoring and scanning: Continuously check systems for vulnerabilities
6. Test, document, and implement patches: Apply patches after testing and track changes
7. Audit and report: Review patch effectiveness and communicate results to stakeholders

Why is this solution effective in mitigating malware?

Patch management is effective in mitigating malware by ensuring that software vulnerabilities are promptly addressed, thereby reducing potential entry points for malicious attacks. As noted by the National League of Cities, "Good cybersecurity hygiene includes keeping all software up to date with the latest patches. This practice is fundamental to reducing your attack surface and mitigating the risk of ransomware infections."

* Blacklisting

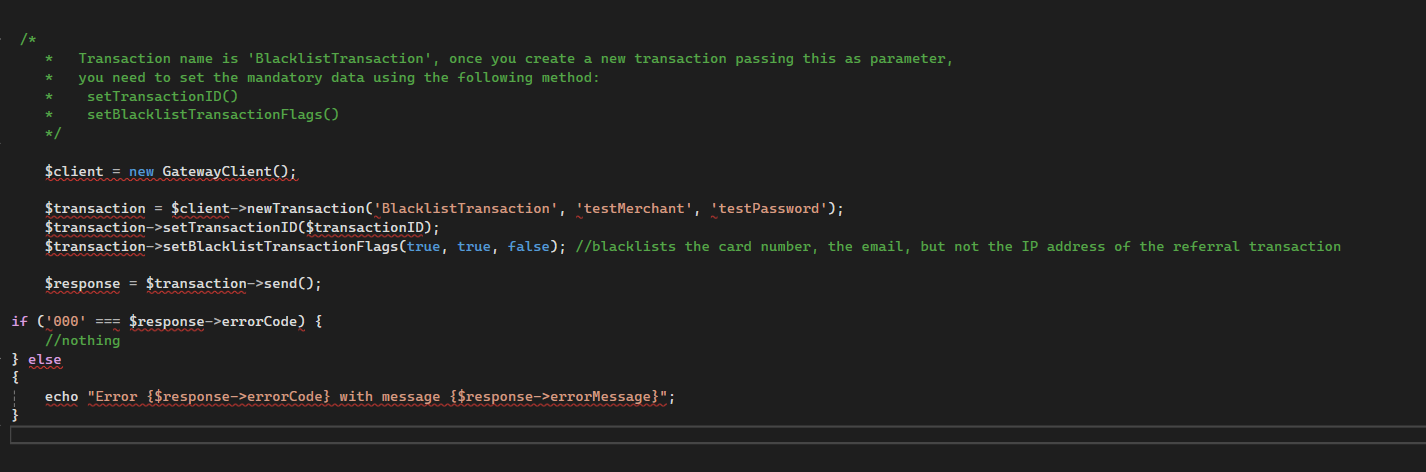
Implementation:

1. Set a list of the response codes that are going to be blacklisted
2. Set a blacklist policy for a certain type of transaction. The policy can be set at the following levels:

* at the portfolio level - if the blacklist policy has to be enabled for all the merchants under a particular portfolio; when set, the settings are applied to the new merchants only.
* at the reseller level - if the blacklist policy has to be enabled for all the merchants under a particular reseller; when set, the settings are applied to the new merchants only.
* at the merchant level - if the blacklist policy has to be enabled for a particular merchant.

1. Check which transactionID has been blacklisted

Example Code:



Why is this solution effective in mitigating malware?

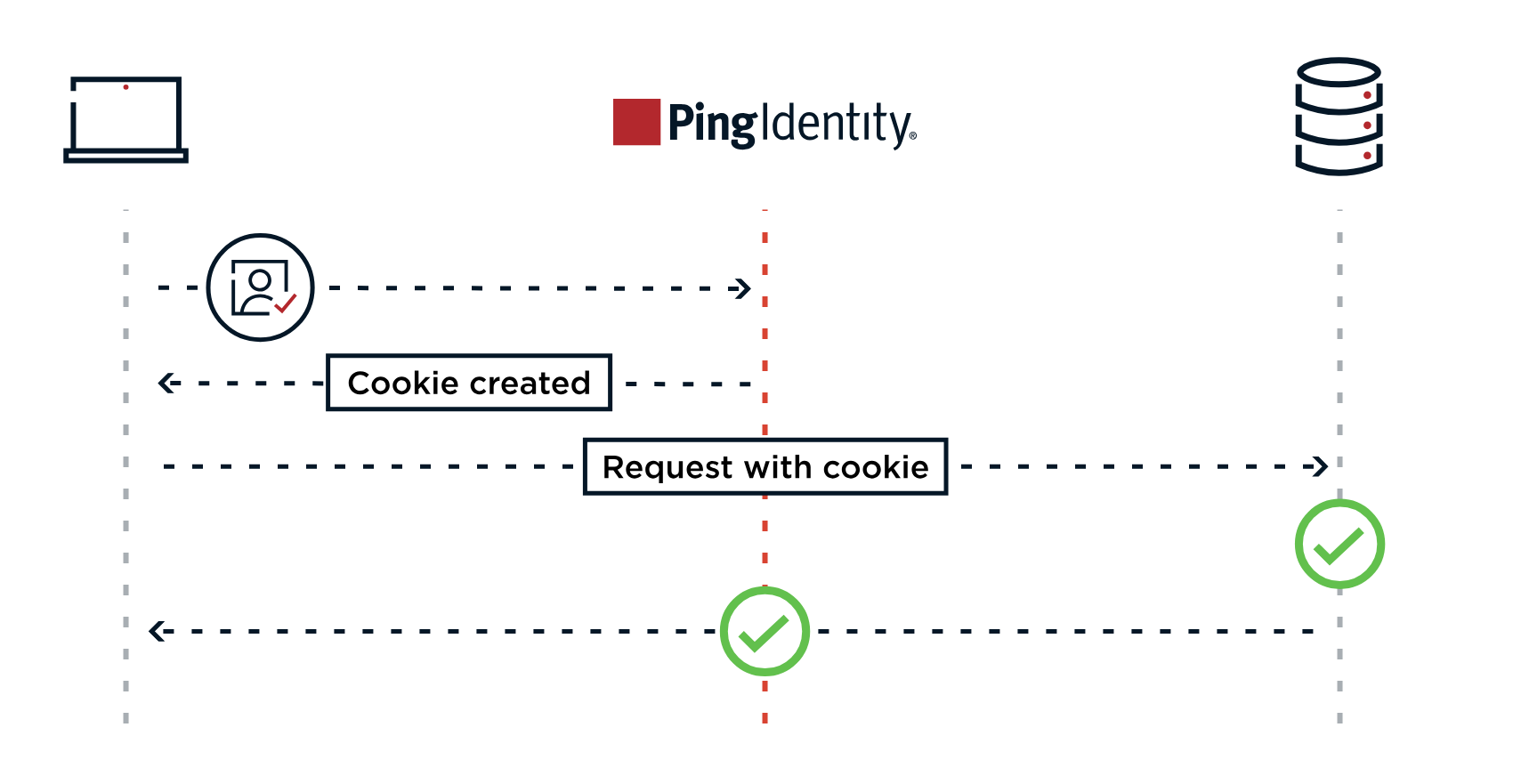
1.3 Session Hijacking

Description: The Session Hijacking attack consists of the exploitation of the web session control mechanism, which is normally managed for a session token.

Mitigation Techniques

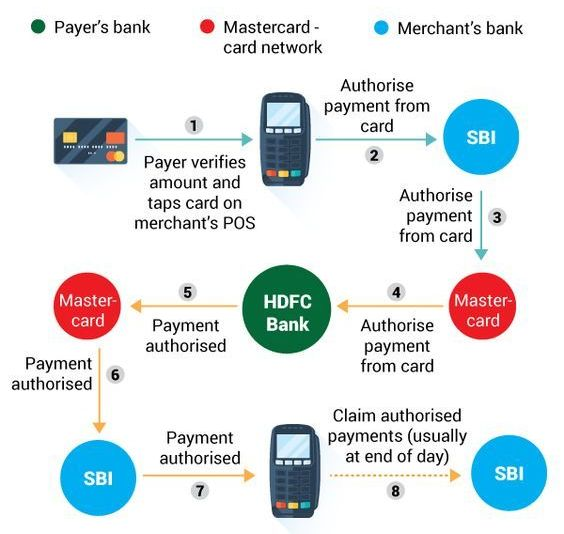
* Session Management

Implementation:

1. Identifying the session management requirements which are suited for the payment gateway and user experience objectives, such as session timeout policies
2. Choosing an appropriate session storage location
3. Establishing secure user authentication methods, such as multi-factor authentication, username-password combinations, etc.
4. Implementing a secure session ID generator
5. Managing and storing session IDs securely with cookies, URL parameters, etc.
6. Configuring cookie settings with the appropriate security attributes
7. Defining incidents or actions when a user session can be revoked

* Multi-Factor Authentication

Implementation:

1. Assess Security Needs: Identify risk levels associated with the business and the types of transactions that require added security. For instance, if the business deals with large or high-value transactions, implementing MFA for every transaction may be necessary
2. Choose MFA Methodology: Select MFA methods that suit the business model and customer base. For e-commerce sites, 2FA via SMS or email may be convenient, while financial platforms may benefit from biometric verification.
3. Integrated MFA with your payment system: Work with yout payment processor to integrate MFA into your existing payment platform. Ensure that the MFA setup is compatible with mobile devices, as many customers complete online transactions via smartphones
4. Conduct User Testing: Test the MFA process with a group of users to identify potential issues and ensure a smooth experience. Gather feedback to refine the process and eliminate any points of friction.
5. Educate and Support Customers: Inform customers about the new MFA feature, explaining how it protects their data and prevents fraud. Offer customer support to assist users who may need help navigating the new process.
6. Monitor and Update Regularly: Regularly monitor MFA performance and adapt to emerging threats by implementing new authentication factirs or enhancing existing protocols.

***Data Encryption and Archival***

* *Security Issues*

2.1 Data Exfiltration

Description: Data exfiltration typically involves a cyber criminal stealing data from personal or corporate devices, such as computers and mobile phones, through various cyberattack methods. A common data exfiltration definition is the theft or unauthorized removal or movement of any data from a device.

Mitigation Techniques

* Penetration Testing

Implementation:

1. Planning

* The planning phase involves determining the test’s objectives and performing initial system reconnaissance. The pen tester gathers information during this state, often using social engineering to obtain the data needed to perform the attack.

1. Scanning

* The planning phase involves analyzing or scanning the system to determine how it will respond to the attack. Pen testers often use technical tools during this process, performing vulnerability scans and looking for gateways to gain unauthorized access.

1. Breaching

* The breaching phase involves using various strategies, such as SQL injection and backdoors, to identify a way to bypass the firewall and breach the system. The pen tester can then breach the system, taking control of devices or the network or extracting data.

1. Burrowing

* The burrowing phase involves determining how long the pen tester can stay in the system, identifying data they can compromise, and learning how much deeper the tester can burrow into the system. The pen tester strives to maintain access for as long as possible, often by installing backdoors and planting rootkits.

1. Analyzing

* The analyzing phase involves creating a detailed configuration review and reporting the test results. Additionally, the pen testers may simulate how a malicious actor will try to cover their tracks. At the end of the test, the pen tester gathers all the information obtained and reports or exploitable vulnerabilities.
* Intrusion Detection and Prevention System (IDS/IPS)

Implementation:

1. Define Network Segmentation

* Identifying Critical Assets: Identifying critical assets such as servers containing sensitive data, customer information databases, or proprietary software systems within the network. Understanding what needs protection is the first step in effective security.
* Creating Segmentation Zones: Following the first step, one should create network segmentation zones. These zones group assets with similar security requirements. For example, there may be a zone for customer data servers and another for public-facing web servers. This segmentation is crucial for controlling and monitoring network traffic effectively.

1. Selecting the RIght Hardware and Software

* Hardware Requirements: To carefully choose the hardware that will host one’s IDS/IPS solution. Factors to consider include processing power, memory, network interfaces, and storage. Ensure that the hardware can handle the expected traffic load and scale as needed.
* Software Requirements: Select IDS/IPS software that aligns with your organzation’s requirements. Consider open-source solutions like Snort or commercial products like CIsco Firepower. Evaluate features, scalability, and support option when making a decision.
* Compatibility Checks: Before installation, verify that the chosen IDS/IPS solution is compatible with the existing network infrastructure and security tools. Incompatibilities can lead to functionality issues that may compromise security.

1. Installation and Configuration

* Deploying IDS/IPS Sensors: Installing key sensors at key points in the network segments or at entry/exit points would capture and analyze network traffic for suspicious activity. Proper sensor placement isis essentidal for effective threat detection.
* Configuring Network Taps or SPAN Ports: Ensure that the sensors can access the network traffic it needs to monitor. Use network taps or SPAN (Switched Port Analyzer) ports to mirror traffic to the sensors without disruption network operations.
* Initial Setup and Configuration: Follow the installation and configuration guidelines provided by one’s IDS/IPS vendor or open-source project. Configure network interfaces, set up alerting mechanisms, and establish initial rules or signatures.

1. Rule and Signature Management

* Fine tuning Detetcuon Rules: Customize detection rules to align with the network’s specific characteristics and threate landscape. Regularly review and adjust rules to reduce false positives and increase detection accuracy.
* Updating Signatures and Rules: Stay up-to-date with the latest threat intelligence by regularly updating signatures and rules. This ensures the IDS/IPS can detect emerging threats effectively.
* Customization for the Environment: Tailor the IDS/IPS to the organization’s needs. Customize alerting thresholds, response actions, and reporting to align with the security policies.

2.2 Insider Threats

Description: Insider threat is the potential for an insider to use their authorized access or understanding of an organization to harm that organization.

Mitigation Techniques

* Least Privilege

Implementation

1. Carry out a privilege audit: Perform a through audit of the full environment to ensure that all privileged accounts are under policy management. Include privileged accounts and credentials held by employees, contractors, and third-party vendors, whether on-premises, over remote access, or in the cloud. The audit should cover both human and machine identities, including those in DevOps workflows, with special attention on default and hard-coded credentials that organizations frequently overlook.
2. Establish least privilege as the default: Grant all new accounts the minimum privilege needed to perform the job. Remove or reconfigure default permissions on new systems or applications. Zero standing privileges should be one’s goal, where feasible. Using role-based access control can help one determine which privileges a new account requires by control can help one determine which privileges a new account requires by setting general guidelines around a responsibility, task, or team. Be sure to adjust permissions as a user’s role changes to avoid privilege creep.
3. Implement separation of privileges: Avoid over-provisioning by restricting local administrator privileges. Separate administrative accounts from standard accounts, even for the same user, and isolate privileged user sessions. Grant higher-level system functions (read, write, execute) at the minimum level required. Additionally, divide auditing and logging capabilities. Host the session logs outside of the database monitored and restrict write access for log admins.
4. Provide just-in-time, granular access: To maintain least-privilege access without impending employee workflow, supplement role-based access control with time-based privileges. Replace hardcoded credentials with dynamic secrets or implement one-time-use (or disposable) credentials. This allows one to temporarily elevate access permissions without causing privilege creep in cases where a user requires increased authority to carry out a specific task or a short-term project.
5. Monitor and analyse privileged access: Continuously log and monitor authentications and authorizations to systems throughout the network. Ensure that individual actions are traceable. Capture all keystrokes, RDP, and SSH sessions, and use automation tools to detect anomalous activity and slert you to potential problems.
6. Review privileges regularly: The company should define a cadence to review existing account and permission levels. Newer companies should hold a monthly review, while mature companies with more accounts o manage can host a quarterly review. Revoke any excess privileges you discover, and close or deprovision all inactive accounts.

* Data Loss Prevention

Implementation

1. Scope the program

* Goal: Provide insight into data and business practices to allow DLP to address real issues without prompting disruption
* First, understand the needs of the business by identifying and prirotizing risks such as the data risk appetite. Then identify the data the business needs to protect, including intellectual property (IP), and verify the data and application owners.
* Use data flow mapping to identify where the data originates, where it is being saved and where it is going. For example, data that it downloaded from a server, saved to a desktop, sent via a web browser or uploaded to a cloud app has a data flow, and you use DLP tools to detect and block data at all of these points. Finally, develop appropriate security and information policies to support and promote the DLP program.

1. Start awareness and governance activities

* Goal: Build a plan to communicate to all parties what is happening with the data, why it is happening , the benefits, and the likely impacts on them.
* Identify and improve business practices for data handing. For example, create a list of accepted protocols, programs and data-handling procedures, and work with legal and procurement teams to include data loss requirements in contracts. Because DLP needs constant iteration as business needs change, the communication lines must remain open. Use a collaboration platform to perform surveys, convey messages and give users the ability to ask questions.

1. Design initial architecture

* Goal: Map the DLP use cases (detection and context requirements) to each enforcement point.
* Identify the DLP tool types that will provide the necessary control. As it’s not always possible to get one vendor or solution to cover every aspect of DLP your business may need, choose vendors that can protect data in the multiple use cases identified in the data flow mapping activity. It’s also worth testing each solution thoroughly as a proof of concept before making a selection, and ensuring that it meets business requirements.

1. Begin to address dependencies

* Goal: Push for improvements on some of the dependencies identified early on
* The ability of DLP programs to detect data loss can be confused by a range of dependencies, both technical and procedural. DLP effectiveness depends on addressing these dependencies.
* Take identity management, for example. DLP cannot do much to prevent data loass if users are granted unrestricted access to data by default. Ensure that one only provides access to data if there is a legitimate business need. Also use data classification, which discovers sensitive data in storage locations, such as file shares, cloud storage, databases and network-attached storage appliances, to shed ligh on data permissions.

1. Deploy, operate and evolve

* Goal: Start small and deploy in stages, as DLP rollouts can be disruptive.
* Use a “monitoring only” initial implementation so one can test and refine the policies to reduce both false negatives and business impacts. Communicating each stage to impacted users, and let them know what is happening with data, when and why.
* As one moves into operations mode, identify operational metrics that support both continuous delivenry improvement and measuring DLP’s impact on data risk. These metrics could include the number of resolved incidents or the number of times DLP blocked sensitive data.
* DLP is not a set-it-and-forget program, so be sure to allocate some resources to fine-tune DLP policies as changes in business processes or data types occur.

2.3 Backup Data Corruption

Description: Backup data corruption is a serious problem that can compromise your ability to restore your systems and files in case of a disaster. It can happen due to various reasons, such as hardware failures, software bugs, network errors, human errors, malicious attacks, or environmental factors.

Mitigation Techniques

* Redundant Array of Independent Disks (RAID)

RAID is a storage technology that combines multiple disk drive components into logical unit for the purposes of data redundancy and performance improvement. RAID is a form of data storage virtualization technology that integrates multiple disk drives into a single logical unit.

Implementation

Before diiving into the setup process of a RAID Array in Windows 10, these are the common raid levels:

* Raid 0 (Striping): Improves performance by spreading data across multiple drives, but offers no redundancy. RAID 0 offers no protection against disk failure, making it best for non-critical data where speed is the priority.
* RAID 1 (Mirroring)**:** Provides data redundancy by creating an exact copy of data on two drives. Ideal for critical data that needs a backup.
* RAID 5 (Striping with Parity)**:** Offers a balance of performance and redundancy, requiring at least three drives. Good for businesses that need both speed and data protection.
* RAID 10 (Mirroring and Striping)**:** Combines the benefits of RAID 1 and RAID 0, requiring at least four drives. Excellent for environments that need high performance and strong data protection.

Windows 10 includes built-in tools for setting up software RAID. Here’s how to configure RAID and different RAID levels:

### *Prerequisites*

* At least two hard drives for RAID 0 and RAID 1, utilizing multiple disks for enhanced performance and redundancy
* At least three hard drives for RAID 5
* At least four hard drives for RAID 10
* Administrator access to your Windows 10 PC

### *Configuring Raid 0 or Raid 1*

1. Press Windows Key + X and select “Disk Management.”
2. Right-click on the disk the user wants to use and select “New Striped Volume” for RAID 0 or “New Mirrored Volume” for RAID 1. RAID 1 mirrors the same data on two drives, ensuring data security through fault tolerance and redundancy.
3. Follow the wizard, selecting the disks the user would want to include in the array.
4. Choose a drive letter and format the new volume.

### *Configuring Raid 5*

1. Open the Start menu and type “Storage Spaces,” then select “Manage Storage Spaces.”
2. Click “Create a new pool and storage space.”
3. Select the drives the user wants to include in your RAID 5 array and click “Create pool.”
4. Under “Resilience type,” select “Parity.”
5. Choose a size for the user’s storage space and click “Create storage space.”

After the setup, users will see a single disk in Windows Explorer, indicating the successful configuration of the RAID storage pool.

### *Configuring Raid 10*

1. First, create two RAID 1 arrays following the steps for RAID 1 above.
2. Once user has two mirrored volumes, go back to Disk Management
3. Right-click on one of the mirrored volumes and select “New Striped Volume.”
4. Add the second mirrored volume to this striped volume.
5. Format the new volume to complete the RAID 10 setup.

RAID 10 provides redundancy, ensuring data is safe even if a disk fails.

* Checksums

Implementation

1. Calculate the Checksum**:** Use a checksum algorithm (e.g., CRC, MD5, SHA-256) to calculate a checksum for the data user wants to verify.
2. Store or Transmit the Checksum: If you're verifying data integrity over a network or storing data, you'll need to transmit or store the calculated checksum along with the data.
3. Retrieve the Data**:** When you want to verify the integrity of the data, retrieve the data along with the stored checksum.
4. Recalculate the Checksum**:** Use the same checksum algorithm to recalculate the checksum for the retrieved data.
5. Compare Checksums**:** Compare the recalculated checksum to the stored checksum. If the checksums match, the data has not been altered or corrupted. If they do not match, it indicates that the data has been modified or corrupted in some way.
6. Take Action**:** Depending on the application, you may take different actions when the checksums do not match. For example, in network communications, you might request the data to be retransmitted. In storage systems, you might initiate a data recovery process.

### 

References:

<https://ibm.com/think/topics/data-breach#:~:text=A%20data%20breach%20is%20any,is%20also%20a%20data%20breach>.

<https://www.checkout.com/blog/payment-tokenization>

<https://baffle.io/data-tokenization/>

<https://stripe.com/en-sg/guides/pci-compliance>

[https://basyspro.com/solutions/pci-compliant-payment-gateway](https://basyspro.com/solutions/pci-compliant-payment-gateway/?utm_source=chatgpt.com)

<https://www.microsoft.com/en-gb/security/business/security-101/what-is-malware#:~:text=about%20Microsoft%20Security-,Malware%20defined,extort%20payment%20information%20from%20victims>.

<https://kirkpatrickprice.com/blog/10-ways-to-conduct-patch-management/>

<https://www.nlc.org/article/2023/11/29/patching-a-necessity-in-a-world-of-ransomware>

<https://unipaygateway.info/tutorials/15&t=1>

<https://developers.payzone.ma/gateway/transactions-blacklist>

<https://owasp.org/www-community/attacks/Session_hijacking_attack>

<https://www.pingidentity.com/en/resources/blog/post/session-management.html#How-to-Implement-User-Session-Management>

<https://www.linkedin.com/pulse/how-implement-multi-factor-authentication-mfa-online-julia-fernandes-nc8jc>

<https://www.fortinet.com/resources/cyberglossary/data-exfiltration#:~:text=Data%20exfiltration%20typically%20involves%20a,any%20data%20from%20a%20device>.

<https://www.bluevoyant.com/knowledge-center/penetration-testing-complete-guide-to-process-types-and-tools#what-are-the-main-steps-of-penetration-testing>

<https://www.linkedin.com/pulse/6-step-implementation-guide-ids-ips-proinfinc>

<https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats#:~:text=Negligence%20%E2%80%93%20An%20insider%20of%20this,%2C%20desirable%20travel)%20or%20termination.>

<https://www.strongdm.com/blog/principle-of-least-privilege>

<https://www.gartner.com/en/articles/build-a-successful-data-loss-prevention-program-in-5-steps#:~:text=DLP%20Step%20%231:%20Scope%20the%20program&text=First%2C%20understand%20the%20needs%20of,the%20data%20and%20application%20owners.>

<https://www.linkedin.com/advice/0/what-common-causes-consequences-backup#:~:text=Backup%20data%20corruption%20is%20a,malicious%20attacks%2C%20or%20environmental%20factors.>

<https://www.hp.com/us-en/shop/tech-takes/how-to-set-up-raid-windows-10-pc>

<https://www.geeksforgeeks.org/understanding-checksum-algorithm-for-data-integrity/>