Module 3: Data Security Measures and Incident Response

Learning Outcomes:

- How to Implement data security measures tailored to Truehost's hosting and registrar services.
- How to Develop an incident response plan that meets the Kenya Data Protection Act’s breach reporting requirements.

Truehost’s Security Framework

Truehost employs a multi-layered security approach to safeguard infrastructure and client data. This framework covers various hosting environments, including cPanel, VPS, and Plesk servers, ensuring compliance with the Kenya Data Protection Act and global best practices.

1. Securing cPanel Servers and Client Accounts:

- **Account Isolation:** Truehost uses **CloudLinux CageFS** to isolate each hosting account, preventing one compromised account from affecting others.
- **Secure Access:**

    - Mandatory SSL/TLS encryption for all cPanel sessions.
    - Enabling **Two-Factor Authentication (2FA)** for client accounts to protect against unauthorized access.
    - Security Question for the Truehost Client Area.
- **Automated Threat Detection:**
    - **cPhulk Brute Force Protection** blocks repeated login attempts from suspicious IP addresses.
    - **ModSecurity** prevents exploitation of web application vulnerabilities.

2. Securing VPS Servers:

- While Truehost does not directly offer security patches to VPS servers, we proactively guide and provide measures to be taken by clients/customers so as to secure their VPS servers.

3. Securing Plesk Servers:

- Implementing Plesk's built-in **Fail2Ban** intrusion prevention system to block malicious IPs.

- Enforcing strong password policies for all user accounts.
- Configuring backups to protect sensitive data.

4. Implementing Secure Protocols (SSL/TLS on Truehost-hosted Websites):

- Truehost provides free SSL certificates for all hosted domains through **Let's Encrypt**.
- Automatic HTTPS redirection ensures secure data transmission between websites and their users.
- Regular SSL certificate checks to prevent expired certificates from compromising security.
- Automatic issuance and renewal of the free SSL certificate that is provided by default on the shared hosting servers.

Preventing Cybersecurity Threats at Truehost

1. How Does Truehost Mitigate Security Risks?

- **Imunify360:** An advanced security solution that provides:
  - Malware scanning and removal.

- **CloudLinux CageFS:** Isolates hosting accounts, creating a virtualized environment to prevent cross-account contamination.
- **SSL/TLS:** Ensures all data exchanged between servers and users is encrypted.
- **2FA:** Adds an extra layer of security for both client and administrator accounts. By default 2FA is enabled on cPanel accounts.
- Customers can enable 2FA to prevent unauthorized access thus protecting their data from being compromised or accessed without their approval.

- **Firewalls:** Block unauthorized access and protect against intrusion attempts.
- **cPhulk Brute Force Protection:** Limits brute-force login attempts and blacklists malicious IPs.

2. Securely Storing Billing and Payment Data:

- Compliant with **PCI DSS** (Payment Card Industry Data Security Standard).
- Limited access to payment systems, ensuring only authorized personnel can view sensitive information.

Incident Response.

1. What Steps should be Taken?

- **Preparation:** Incident response plans should be reviewed and updated regularly. Teams should be trained to respond swiftly to security events.
- **Detection:**
  - Continuous monitoring.
  - Log analysis to identify suspicious activities.
- **Containment:**
  - Isolate affected servers or accounts.
  - Temporarily disable compromised systems to prevent further damage.

2. Steps to Detect and Contain Breaches:

- Identify compromised files or systems.
- Use automated tools to quarantine malware or affected processes. (e.g immunify 360)
- Perform root-cause analysis to understand the origin of the breach.

3. Reporting Breaches:

- It is required to notify relevant regulatory bodies (e.g., Kenya Data Protection Commissioner) within required timelines in case of major breaches.
- Document all actions taken, including timestamps, for compliance audits.

4. Notifying Affected Truehost Clients:

It is also required to notify the affected customers indicating what happened, the steps being taken to address the issue or if the issue has been addressed, how to identify and mitigate the issue as well.

- Example: [SECURITY ADVISORY] Phishing Email Campaign Notification
  - A detailed advisory was published to warn customers of a phishing email campaign claiming to be from Truehost. The advisory outlined:
    - What the phishing email looked like.
    - How to verify legitimate communication from Truehost.
    - Steps clients should take to secure their accounts.
      (Reference Link)

Outcome:
Enhanced security protocols, updated user guidelines, and

improved incident response processes and secure systems.
