1st Annual University ICT directors Forum – April 10, 2015

Web-hosting & cyber-security challenges

Peter Muia

Senior Systems Administrator – KENET

pmuia@kenet.or.ke

Agenda

- Current Hosting Plan
- Current Hosting Challenges
- Cyber Security threats
- KENET CERT
- Proposed Hosting plan
- QA

Current Hosting Plan

- Shared virtual server – Each university is allocated 20 GB storage with unlimited subdomains and databases but no email services.
  - Centos Linux Server with Cpanel
  - Mysql Database
  - Backups
- Mostly dynamic websites using Content Management Systems (CMS)
  - Popular CMS are Joomla, Drupal and wordpress

Current Hosting Challenges

- Cyber Security – Next Slide
- Exponential growth of the websites in size and number
  - This becomes a challenge when restoring backups
- Websites not properly maintained and lack of action when communication is done on vulnerable websites
- Shared environment
  - Malware infections or security issue affecting one website on shared server can pose potential threat to other sites on the shared service
  - In the event of a cyber security attack, then restoration could take longer depending on the number of other websites that need to be restored
  - The way that CPANEL is implemented for shared hosting is sometimes a source of vulnerabilities
  - The shared server is not scalable for institutions with large and interactive websites

Cyber Security threats

- SQL Injection
- Cross site scripting
- Website defacement
- Phishing
- Denial of Service (DDOS)
- Trojan Horses (Free Modules & Components)
- Exploitation of Known vulnerabilities

Cyber Security Threat Mitigation

- Application Firewall - (DDOS, SQL Injection, Cross-site Scripting)
- Server Hardening – Ports, access etc
- Regular Scanning for vulnerabilities
- Penetration Testing
- Proactive communication with webmasters and ICT directors
- KENET CERT

KENET CERT

- CERT (Computer Emergency Response Team)
- Web Scanning Results are shared to specific webmasters & ICT directors
- Known Vulnerabilities from other CERTS are shared to the Community
- KENET CERT Portal https://cert.kenet.or.ke
  - Vulnerabilities
    - CMS – Drupal, Joomla, Wordpress
    - OS – Debian, Ubuntu, Windows
    - Cyberoam
    - Microsoft
  - Tips and alerts
  - Simple Howts eg How to setup modsecurity

Proposed Hosting Plan

- Dedicated virtual server with a 2.3 GHz CPU speed, 2GB of RAM and 50GB of storage.
- Offer letters sent to 10 ICT directors
- University Responsibility
  - Choice of the Operating System & Updates
  - Regularly updating applications
  - Regularly updating the CMS & plugins
  - Daily or regular updates of the content of your website
  - Ensuring security of the virtual server and applications hosted on it
- KENET Responsibility
  - CERT services
  - Regular vulnerability scans
  - Ensure server uptime

Questions

kenet
Kenya Education Network

Transforming education through ICT

Thank You

www.kenet.or.ke
Jomo Kenyatta Memorial
Library, University of Nairobi
P. O Box 30244-00100, Nairobi.
0732 150 500 / 0703 044 500