RISA

Rwanda Information Society Authority

Directives on Cyber Security for Network and Information Systems for all Public Institutions

June, 2018

Document Title : Directive on Cyber Security for Network and Information Systems

Issue/Version No : 1.0

Issue Date : June 11, 2018

Change History:

Date	Issue No.	Details of Changes
June 11th 2018	1.0	This is the first issued Directive for Cyber security for Network and Information

Issued by:

Rwanda Information Society Authority (RISA)

Contact Person:

Roger Cyiza USENGIMANA
Ag. Division Manager | Rw-CSIRT
RISA-IT Security Division
Phone: +250 788 856653
Email: roger.cyiza@risa.rw
roger.cyiza@rdb.rw

Table of Contents

Purpose of the Directive 4

I. Minimizing the Exposure of Systems to External Networks 4

II. Intrusion Prevention System (IPS) 4

III. Email Protection 5

IV. Gateway Level Antivirus Protection 5

V. Wireless Protection 5

VI. Web Browsing Protection 5

VII. Securing On-premises Hosted Services 5

VIII. Visibility and Monitoring 6

IX. Patch Management 6

X. Security Assessment 7

XI. End User/End Point Protection 7

XII. Implement Passwords Policy 7

XIII. Availability of Systems and Services 7

XIV. Backups 8

XV. Incident Management 8

XVI. Security Awareness 9

Purpose of the Directive

This Directive aims at providing important instructions and guidelines for securing GoR entities ICT infrastructures and Information by:

- ➢ Strengthening ICT infrastructure and information access.
- ➢ Insuring high availability of data and systems for dedicated services
- ➢ Protecting against malware and other related threats which can compromise the confidentiality, integrity and availability of data

To achieve the above, all GoR entities should have minimum security controls implemented within their network before connecting their network to Internet. These controls are described below:

I. Minimizing the Exposure of Systems to External Networks

- Install and configure Gateway firewall
- Configure Inbound and outbound ACL (Access Control List) to control only required and legitimate traffic only to be allowed to go In and Out of the network.
- Close all the ports and only open the required port
- Avoid "any""any" rules set up in all the configurations
- All rules must be configured to ensure no 'unwanted services' or 'hosts' are exposed to the internet
- Implement network segregation by having DMZ for public facing servers, Server Zone and User zone
- Ensure that the network is secure by Segregating different administrative duties
- All remote access to core ICT infrastructure should be done via VPN

II. Intrusion Prevention System (IPS)

- Implement IPS at gateway for all incoming and outgoing traffic to detect and prevent any intrusion or threats
- Configure intrusion protection system to protect against denial of service attacks or any malicious attacks

III. Email Protection

- You must ensure that all the mails are scanned before entering into network / email server and Antispam / Antivirus system

Implement Policy based Data leak protection solution to protect sensitive data leaving out of your network through emails

IV. Gateway Level Antivirus Protection

- You must have gateway level antivirus protection to detect and disinfect the network traffic to ensure all detectable virus on the gateway not entering and infecting internal servers or systems

V. Wireless Protection

- Wi-Fi must be secured by setting wireless hotspots using proper authentications and strong password or key
- No wireless networks should be connected to their internal network directly. They must be connected through firewall.

VI. Web Browsing Protection

- You must implement a web proxy to protect end users from web threats and control their time online
- You must apply URL-filtering policies and enforce browsing quotas and time-based web surfing for individual users or groups to limit the use of unwanted applications or services while giving priority to business-critical resources

VII. Securing On-premises Hosted Services

- You must harden web servers and apps ensuring minimum secure application are hosted
- Every web services MUST be SSL certificate enabled

- Thoroughly test the web-based application for any security flaw using guidelines from Open web application security project OWASP (shared separately) and published on RISA website
- You must implement security controls like reverse proxy authentication which provides an added layer of security for enterprise applications
- Every web application MUST be controlled by a web application firewall for more security of web services.
- All the internet facing server MUST be placed in the DMZ
- You must segregate development/testing environment/activities from production environment/activities

VIII. Visibility and Monitoring

- Design and implement network to have clear visibility of the traffic going between:
  - Computer to computer
  - Computer to Server,
  - Server to Computer,
  - Server to Internet and
  - Internet to Internal server and Computers.
- Use 'Static IP addressing' on systems and servers recorded with system identifier to facilitate identification of intruders into the network by enabling logs and alerts and take appropriate steps to stop any threats and anomalies.
- Enable alert by Mail or SMS to communicate any issues that arise
- Whenever help is needed contact National CSIRT to manage the incidents

IX. Patch Management

- All the system and application MUST have latest patch installed
- Test the patch before applying and then apply in the production environment
- Patch network devices (Firmware), applications, middleware, OS and any utility programs (Office, Adobe etc...)

X. Security Assessment

- You must carry out Regular vulnerability scanning to ensure all the known vulnerabilities such as bugs and configurations are identified
- All the identified vulnerabilities MUST be fixed by patching the systems or applications immediately and proper systems and network reconfiguration must be done.
- After fixing the identified vulnerabilities conduct internal and external penetration tests to ensure no known vulnerability are left unattended to within the ICT infrastructure and services.

XI. End User/End Point Protection

- Install End-Point Protection to secure all the end points such as Host based IDS / IPS for servers
- Ensure that end user devices, systems and application are protected using Endpoint protection and Antivirus solutions.

XII. Implement Passwords Policy

- Strictly use strong passwords:
  - Minimum 10 character
  - Combination of Alpha numerical and special characters
- Don't reuse the passwords
- Have different passwords for different accounts
- Change all default passwords upon installation of new software or new OS
- Limit failed login attempt to three times and then lock the user
- Set up a two-factor authentication for critical applications and/or systems

XIII. Availability of Systems and Services

Ensure critical services are available whenever it required by:

- Having Redundant System components

- Redundant Servers
- Failover networks
- Disaster Recovery Arrangements Such as alternative site or arrangements based on the criticality of the services they render
- Disaster Recovery infrastructure should be tested regularly; All Process and Procedures should be documented.

XIV. Backups

- All the GoR Entities should have backup:
  - Daily
  - Weekly
  - Monthly and
  - Yearly
- One copy of backup should be stored at offsite securely
- All the backup should be encrypted with password
- Backup should include data, applications, configurations and Systems
- Restoring from backup exercise should be tested and documented

XV. Incident Management

- Have a clearly defined incident management procedure (refer to the Incident management procedure circulated).
- Every Institution should establish an Incident management team and clear communication channel internal or external for communicating the incidents
- Every institution must Classify incidents level of severity: Major, Medium and Minor
- Establish procedures for handling the incident according to the classification and follow it strictly
- For any Cyber security related incident all institution MUST contact National CSIRT

XVI. Security Awareness

- Conduct regular security awareness programs for the end-users and system administrators to secure institution's data and information from any attacks