BOTSWANA COMMUNICATION REGULATORY AUTHORITY

DRAFT

GUIDELINES ON ELECTRONIC MAIL (E-MAIL) SECURITY

Reviewed by

Position	Chief Technology Officer
Name	Mr. Tshoganetso Kepaletswe
Signature	
Date	

Approved BY

Position	Chief Executive
Name	Mr. Martin Mokgware
Signature	
Date	

Table of Contents

1 Introduction..... 3

2 Terms and definitions 4

4. AUDIENCE AND ASSUMPTIONS 4

5. COMMON EMAIL VULNERABILITIES AND THREATS 4

6. SECURITY SAFEGUARDS 6

7. ENCRYPTION RELATED STANDARD 8

9. REVIEW 11

1 Introduction

1.1 Electronic Mail (E-mail) is the most popular system for exchanging information over the Internet or any other computer network. After Webservers, mail servers are the hosts on an organization networks that are most often targeted by cyber attackers.

1.2 Securing an e-mail system is the responsibility of an organization's IT department administrators. However, anyone responsible for the confidentiality, integrity, and availability of the information sent via e-mail should be aware of the threats facing e-mail systems and understand the basic techniques for securing these systems.

1.3 E-mail security relies on principles of good planning and management that provide for the security of both the e-mail system and the IT infrastructure. With proper planning, system management, and continuous monitoring, organizations can implement and maintain a safe and secure electronic mail environment.

1.4 E-mail messages are generally sent over untrusted networks outside the organization's security boundary. When these messages lack appropriate security safeguards, they are like postcards that can be read, copied, and modified at any point along these paths.

1.5 Email has several issues which if not properly addressed may lead to unauthorized access to the system files or folders not meant for public access. Email attacks may lead to denial-of-service attacks which deny valid/ legitimate users' access to the system.

1.6 Improperly configured email may lead to unauthorized access and disclosure of sensitive information and data leakage and may be intercepted by hackers (man in the middle attacks).

1.7 With these threats emerging from time to time it is imperative that proper measures are put in place to minimize exposure to them.

2 Terms and definitions

Attack – malicious activities performed by attackers.

Attacker – performs malicious activities to gain unauthorized access and disrupt services

Hackers – Highly skilled attacker that perform unusual malicious activities on computer systems

Target – people that are targeted by hackers or attackers

3. PURPOSE

3.1 The purpose of the Electronic Mail Security guideline is to recommend security practices for designing, implementing, and operating email systems to public and private networks.

4. AUDIENCE AND ASSUMPTIONS

4.1 This document may be used by organizations interested in enhancing security on existing and future email systems to reduce the number and frequency of email related security threats and incidents.

4.2 The target audience of these documents are: -

4.2.1 System engineers - when designing and implementing email systems.

4.2.2 System administrators - administering group email systems.

4.2.3 Programmers, Iinformation Ttechnology (IT) security officers – to ensure adequate security measures have been considered for all phases of the system's life cycle

4.2.4 Users - setting up email clients and accessing email

5. COMMON EMAIL VULNERABILITIES AND THREATS

5.1 Attackers can exploit e-mail to gain control over an organization, access confidential information, or disrupt IT access to resources. Common threats to e-mail systems include the following: -

5.1.1 **Malware:** - attackers are taking advantage of e-mail to deliver a variety of attacks to organizations using malware, or “malicious software,” that include viruses, worms, Trojan horses, and spyware. These attacks, if successful, may give the malicious entity control over workstations and servers, which can then be exploited to change privileges, gain access to sensitive information, monitor users’ activities, and perform other malicious actions.

5.1.2 **Social engineering**. Rather than hack into a system, an attacker can use e-mail to gather sensitive information from an organization’s users or get users to perform actions that further an attack. A common social engineering attack is e-mail spoofing, in which one person or program successfully masquerades as another by falsifying the sender information shown in e-mails to hide the true origin.

5.1.3 **Spam and phishing:** - Unsolicited commercial e-mail, commonly referred to as spam, is the sending of unwanted bulk commercial e-mail messages. Such messages can disrupt user productivity, utilize IT resources excessively, and be used as a distribution mechanism for malware. Related to spam is **phishing,** which refers to the use of deceptive computer-based means to trick individuals into responding to the e-mail and disclosing sensitive information. Compromised e-mail systems are often used to deliver spam messages and conduct phishing attacks using an otherwise trusted e-mail address. A malicious email is sent to victim with the purpose of getting the victim to click on a link. The link will give the attacker access to the victim’s email account or even computer.

5.1.4 **Human Factor -** Unintentional acts by authorized users. Not all security threats are intentional. Authorized users may inadvertently send proprietary or other sensitive information via e-mail, exposing the organization to embarrassment or legal action.

5.1.5 **Denial of Service (Email Bomb)** – Denial of Service (DoS) attack against email servers. This attack's main objective is to make email accounts unusable or even cause a downtime.

5.1.6 **Man-in-the-Middle attack** - An attacker intercepts an email not intended for them, reads and modifies the content of the email and release it to be receive by the recipient.

6. SECURITY SAFEGUARDS

6.1 Management, operational, and technical safeguards are necessary to ensure that the confidentiality, integrity, and availability needs of the mail system, its supporting environment, and the data handled by it are addressed. Several security and best practice frameworks are recommended such as MITRE ATT&CK, NIST and OWASP.

6.2 **Awareness**

6.2.1 Additionally, organizations should implement and deliver security awareness and training, because many attacks rely either partially or wholly on social engineering techniques to manipulate users.

6.3 **Management Controls**

6.3.1 Management security controls-such as organization-wide information security policies and procedures, risk assessments, configuration management and change control, and contingency planning, are essential to the effective operation and maintenance of a secure e-mail system and the supporting network infrastructure.

6.4 **System Hardening**

6.4.1 The most critical aspect of deploying a secure e-mail system is careful planning before installation, configuration, and deployment. As is often said, security should be considered from the initial planning stage, at the beginning of the system development life cycle, to maximize security and minimize costs.

6.5 **Mail Server Security**

6.5.1 Organizations should install the minimal mail server services required and remove unused services, applications, and scripts. Securing the mail server application also includes configuring the mail server user authentication and access and resource controls; configuring, protecting, and analyzing log files; and periodically testing the security of the mail server application.

6.5.2 Mail server security should include a control to protect the confidentiality and integrity of the message is to deploy a secure e-mail solution such as leveraging Public Key Infrastructure (PKI) technology to encrypt and sign the message. Digital rights management and data leakage prevention systems can be used to prevent the accidental leakage and exfiltration of sensitive information.

6.6 **Secure the Transmission**:

6.6.1 Most standard e-mail protocols send by default, user authentication data and e-mail content in the clear text, that is, unencrypted. Sending data in the clear text may allow an attacker to easily compromise a user account, intercept and alter unencrypted e-mails.

6.6.2 At a minimum, most organizations should encrypt the user authentication session even if they do not encrypt the actual e-mail data. Mass emails are sent to the target by an attacker to deny them service, by filling up the target's email storage such that the service is limited or even unavailable.

6.6.3 Organizations should prevent the alteration of emails while in transit from the sender to the recipient server. Misconfiguration can lead to Man-in-the-Middle attack and with such, the recipient server can not verify if the email is from the sender.

6.7 **Authorization:**

6.7.1 Email authentication is necessary to authorize which mail server can send emails to a domain. Lack of this can enable attackers to spoof domains and even use them for phishing which leads to a poor reputation score for the organization sending the email.

7. ENCRYPTION RELATED STANDARD

7.1 The two primary email standards for securing email content end-to-end are Pretty Good Privacy (PGP) and Secure Multipurpose Internet Mail Extensions (S/MIME). Both are based, in part, on the concept of public key cryptography, which involves a user having a pair of related keys: a public key that anyone can hold, and a private key that is held exclusively by its owner. OpenPGP is now defined by the Internet Engineering Task Force (IETF) OpenPGP Working Group standard RFC 2440.

7.2 The recipient's public key is used for sending encrypted information that can be decrypted only with the private key. The sender's private key is used for sending digitally signed information whose authenticity can be verified by anyone holding the corresponding public key.

8. GUIDELINES TO FOLLOW

8.1 Appropriate management practices are the most critical to operating and maintaining a secure mail server. These range from development documentation, implementation of policies, standards, procedures, and guidelines that ensure confidentiality, integrity, and availability of information system resources relating to Emails.

8.2 To ensure the security of an email server and the support network infrastructure, the following practices should be implemented: -

8.2.1 Implement logging for system recovery and investigation in the event of an attack.

8.2.2 **Organizational Information System Security Policy:** - A security policy should outline who in the organization is responsible for areas of information security (e.g., Implementation, enforcement, audit, review). The policy should also specify what the basic information system security policies are and their intended internal purpose. The policy must be forced consistently throughout the organization to be effective. Generally, the Chief Information Officers will be responsible for drafting the organization's security policy.

8.2.3 **Configuration/Change Control and Management**—Is the process of controlling modification to a system's design, hardware, firmware and hardware which provides sufficient assurance the system is protected against the introduction of an improper modification prior to, during, and after system implementation. Configuration control leads to consistency with the organization information system security policy.

8.2.4 **Risk Assessment and Management**— Risk management is the process of selecting and implementing of controls to reduce risk to a level acceptable to the organization. It involves determining the

assessment's scope and methodology, collecting, and analysing risk related data, and interpreting the risk analysis results. Collecting and analyzing risk data requires identifying assets, threats, vulnerabilities, safeguards, consequences, and the probability of a successful attack.

8.2.5 **Standardized Configurations**—Organizations should develop standardized secure configurations for widely used operating systems and applications. This will provide guidance to mail server and network administrators on how to securely configure their systems and ensure consistency and compliance with the organizational security policy.

8.2.6 **Security Awareness and Training**—A security training program is critical to the overall security posture of an organization. Making users and administrators aware of their security responsibilities and teaching the correct practices helps them change their behaviour to conform to security best practices. Training also supports individual accountability, which is an important method for improving information system security.

8.2.7 **Contingency Planning, Continuity of Operations and Disaster Recovery Planning** – Contingency planning, continuity of operations and disaster recovery planning are plans setup in advance to allow an organization or facility to maintain functionality.

8.2.8 **Certification and Accreditation**–Certification in the context of information systems security means that a system has been analyzed as to how well it meets all of the Security requirements of the organization. Accreditation occurs when the organization's

management accepts that the system meets the organization's security.

8.2.9 **Implement strict SPF and DKIM policies**

8.2.9.1 Example of deploying a strict SPF

v=spf1 a mx include:spf.xxx.org.bw -all

- \+ ***Pass****, an IP that matches a mechanism with this qualifier will pass SPF*
- \- ***Fail****, an IP that matches a mechanism with this qualifier will fail SPF.*
- ~ ***SoftFail****, an IP that matches a mechanism with this qualifier will soft fail SPF, which means that the host should accept the mail, but mark it as an SPF failure.*
- *?* ***Neutral****, an IP that matches a mechanism with this qualifier will neither pass or fail SPF.*

8.2.9.2 Implement DKIM Policy in line with RFC5863

8.2.10 Implement Multi-Factor Authentication for email accounts and mail server.

8.2.11 Bi-Weekly backup of the mail server

8.2.12 Develop redundancy site for Business Continuity and offsite Backups.

8.2.13 Deploy access control to minimize damage when an account is compromised

9. REVIEW

9.1 The document may be reviewed by the stakeholders and constituents as may be determined from time to time by the Authority.