Today, with the big advancement of technology and the need to share data globally at all time. Security has become one of the most important topics when we talk about data sharing. This means that the more secure and reliable the product is the bigger asset it represents.

Hardware and Software Security

From theory to practice

DaQuan Stevens, Esteban Proano, Salem Alzaabi

Table of Contents

INTRODUCTION

Hardware and software Security represent a big challenge on the current trend of technology, most of the systems used these days handle critical information from clients with complete transparency to the user. This means that were the data is stored, how is being transmitted and who has access to it is beyond the control of the user.

Hardware security is usually seen as the most basic feature of security, it is basically the physical devices that take care of security of a networking system. Then how a business is supposed to structure their network in order to be able to provide a secure service or provide security to themselves. Where severs should be located and how data should be handled. These common issues have been handled by security polices design by groups of big corporations and governments. Record management is one of the big topics together with information governance. These two describe how policies and regulations have been made to ensure some type of "standard" is used throughout the world.

Records are information assets and hold value for the organization. Organizations have a duty to all stakeholders to manage them effectively in order to maximize profit, control cost, and ensure the vitality of the organization. Effective records management ensures that the information needed is retrievable, authentic, and accurate [8].

Software security is the idea of engineering software so that it continues to function correctly under malicious attack. Most technologists acknowledge this undertaking's importance, but they need some help in understanding how to tackle it.

When developing a secure network, the following need to be considered [1]:

1. Access Control – authorized users are provided the means to communicate to and from a particular network.
2. Confidentiality – Information in the network remains private
3. Authentication- Ensure the users of the network are who they say they are
4. Integrity – Ensure the message has not been modified in transit.
5. Non-repudiation – Ensure the user does not refute that he used the network

IT security governance is the system by which an organization directs and controls IT security (adapted from ISO 38500). This system delegates responsibilities to the right person, states who makes decisions and who is accountable   Combining governance and these security steps corporations can build a secure network and secure their assets. For our paper we will describe them and show how an implementation has been done on a corporation.

IT GOVERNANCE

Organizational Structure

Roles and Responsibilities

Strategic Planning

Policy

Compliance

Risk Management

Measuring and Reporting Performance

SECURITY MEASUREMENTS

Access Control

Confidentiality

Authentication

Integrity

Non repudiation

Security policies implemented by Information Security in Abu Dhabi Police

Abu Dhabi Police is General Head Quarters & follows the structure of the Ministry of Interior of United Arab Emirates. Abu Dhabi police duties includes providing the security for Abu Dhabi city (the capital of UAE) and Abu Dhabi, two major cities that are represented in the union of seven state (Abu Dhabi, Dubai, Sharjah, Umm-al-Quwain, Ajman, Ras Al Khaima and Fujaira.

Departments of Information Technology and Telecom

In brief words, Abu Dhabi Police GHQ contains many of sub departments including the department of Information Technology & Telecom which in turn contains number of sub-divisions including Information Security Division.

Information Security Division

The Information Security Division has the responsibility of protecting (system, application, network, users), policy formulation (which provides sufficient awareness and protection from improper use of the technology), audit and monitoring, & implementation of rules and regulation that relate to the information security. This also includes updating the policies and information permanently and continuously to achieve the public interest of the organization.

These policies have been applied as follows;

- **ACCESS CONTROL POLICY**
- ASSET CLASSIFICATION POLICY
- CHANGE MANAGEMENT POLICY
- COMMUNICATION AND OPERATION POLICY
- COMPLIANCE POLICY
- CONFIGURATION MANAGEMENT POLICY
- **CRYPTOGRAPHIC USAGE POLICY**
- **EMAIL SECURITY POLICY**
- HANDHELD AND PDA DEVICE SECURITY POLICY
- INFORMATION EXCHANGE and MEDIA HANDLING POLICY
- (IS)'s ACCEPTABLE USAGE POLICY
- INTERNET SECURITY POLICY
- LICENSE MANAGEMENT POLICY
- **MALICIOUS CODE PREVENTION POLICY**
- NETWORK SECURITY POLICY
- **PASSWORD SECURITY POLICY**
- PERSONNEL SECURITY POLICY
- PHYSICAL AND ENVIRONMENTAL SECURITY POLICY
- SECURITY AWARENESS POLICY
- SECURITY OF THIRD PARTY ACCESS POLICY

In this paper I will be addressing some of these policies, which are in the heart of the subject, and I'm going to select certain points where it cast light on the main points and summarize its content.

ACCESS CONTROL POLICY

Objective:

- The objective of this policy is to control user's access and business processes based on business requirements and security requirements and provide (the information resources) an acceptable level of protection at Abu Dhabi Police (ADP).

Scope:

- The scope of this policy with associated procedures covers all the (IS)'s environments managed by ADP.

ACCESS CONTROL:

- User access to the information resources of ADP will be based on business requirements and specific job responsibilities of the individuals accessing the system and maintaining the infrastructure, software and hardware.
- All Systems should have a user access lifecycle.
- Roles and privileges should be created with the privileges needed for the user.
- User access to information must be controlled base on business requirements and security requirements.
- User access to ADP (IS)'s must be audited to make sure the access of the users is appropriate.
- All Operating Systems and Application must login with a user ID and password. Without entering user ID and password, login must terminate.
- All Equipment on the ADP network must be identified, registered and authorized.

End-user Access Control Policy:

- All users of the ADP (IS)'s should have a unique ID to identify an individual user.
- End users should be presented with a statement of their access rights and required to acknowledge.
- Systems should be configured to remove or disable user accounts after a defined period of inactivity.
- End-users accounts must be approved by the System Owners before being created and enabled.
- If an End-user changes his/her roles within the ADP, their access rights shall be reviewed to ensure they are appropriate.

CRYPTOGRAPHIC USAGE POLICY

Objective:

- Protect the confidentiality, authenticity and integrity of information being stored or transmitted. Cryptographic systems are used for the protection of information that is considered as sensitive information.

Encryption requirements:

- Risk assessment of the business need.
- Business owner should ensure that the requirements of encryption are reviewed and approved by the ADP Information Security team and ADP IT team.
- ADP Information Security team should establish encryption standards for application security, WLAN, file encryption on the basis of the Information System risks.
- ADP should implement the encryption standards as per the business requirements.

Encryption Controls:

- Data transferred through WAN between ADP and its Stakeholders via internet should be adequately protected with suitable encryption.

- Based on business requirements, confidential emails shall be encrypted before sending the same to recipients.
- On basis of business requirements, confidential data should be stored encrypted if necessary.
- Any IT system utilizing encryption for protection of confidentiality of information must be implemented based on approval from ADP Information Security.
- Depending on the business requirements, the asset (information) owner and ADP Security team shall decide a mutually acceptable encryption methodology for protecting identified critical and sensitive business information.

Cryptographic keys shall be:

- Provide adequately protected against unauthorized access.
- ADP Information Security team should have to defined type and quality of encryption algorithm used.
- Digital certificates based on public key infrastructure solutions should be implemented for identified critical applications.
- ADP Staff should be accountable and responsible for the transactions and safe maintenance of the digital certificates.
- ADP Internal Network should have the ability to issue or revoke digital certificates.

EMAIL SECURITY POLICY

Objective:

- To define an acceptable use of ADP email infrastructure and protect the security of information exchanged over emails.

Acceptable Email Usage:

- Access to the email service of ADP will be on basis of business requirements and specific job responsibilities of the individuals.
- All Administrative accounts used for managing the email servers should follow to the ADP Password policy.
- All email User accounts should follow to the ADP Password policy.
- User Account creation should follow a formal approval process.
- Emails from shared accounts should not be routable outside of the ADP network boundary.
- Users must not initiate or forward chain emails from ADP email addresses.
- Spam emails must be reported immediately to ADP Information Security Department through ADP Helpdesk.
- Spoofing and Anonymous is strictly forbidden.

Automated emails:

- Application generated emails must use separate mail infrastructure to ADP users.
- Email Service Accounts used for applications must not be interactive and should follow the ADP Password Policy.

Email Security Controls:

- Only approved ADP mail infrastructure shall be in place, using unauthorized mail relays on the ADP network is explicitly forbidden.
- Public, private key infrastructure shall be used for encrypting emails.
- All email servers shall have a security appliance (Spam Filters, AV Scanners).
- Blocking of suspicious emails shall be performed, with a release process being enabled for legitimate business use mails.

Email Account Auditing

- All official emails shall remain the property of ADP.
- Emails shall be reviewed, monitored, logged with or without the user's knowledge for review against the ADP security policies.

MALICIOUS CODE PREVENTION POLICY

Objective:

The objective of this policy is to describe the requirements for the deployment and use of antivirus software and desktop protection controls on ADP computers to protect electronic information resources within Abu Dhabi Police (ADP) against malicious code attacks.

Scope:

All IT systems and electronic information assets that they contain, that are leased, procured, received, owned, utilized, hosted and/or produced by ADP are covered within the scope of this policy.

Fit for Purpose Anti Malicious Code Infrastructure:

- ADP Management are aware of the importance of preventing network and system disruptions caused by malicious codes such as viruses, worm, Trojan horse etc. and are determined to provide sufficient resources to develop and maintain an anti malicious code structure to prevent any malicious attack.
- The Antivirus infrastructure should be the primary method of control within ADP in preventing disruptions from malicious code. ADP IT team must ensure the antivirus infrastructure is fit for purpose through adoption of leading practice principles for malicious code prevention.

Deployment of Anti Virus and Personal Firewalls:

- All ADP assets such as servers and PCs and workstations should have antivirus application running the current antivirus signatures.
- All PCs and workstations used for accessing production systems should have a personal firewall installed.
- ADP IT team should ensure the antivirus definition is kept up-to-date through an automated distribution process within ADP.
- If a system is too old to use the latest antivirus engine and signatures, it shall be investigated for possible replacement, and mitigating controls used until replaced.

- ADP Staff systems (desktops, workstations) used for such external system access must have the latest antivirus update and personal firewall installed.

Scanning Inbound and Outbound Traffic:

- All Internet traffic coming to and going from Abu Dhabi Police network must pass through dedicated servers and other network devices that perform a Virus-scanning functionality.
- The email server shall quarantine suspicious e-mail and attachments to an isolated storage space for and action review by ADP IT team and release to users.

Virus Signature Updates:

- On daily basis, all virus scanning programs on all systems must be enabled to automatically check the latest update for the antivirus program.
- To ensure coverage and consistent update of antivirus software, all IT systems within ADP must be registered with a centralized domain at ADP.

Systems Hardening and Patching:

- ADP Information Security team and ADP IT team must establish an IT infrastructure patching and a patch management distribution to ensure consistent update of patches for all IT assets within ADP.
- ADP Information Security team must perform periodic audits to review the implementation of minimum security baseline and patch management.

Notification of Users:

- ADP Information Security team should attempt to notify all ADP employees of possible virus threats through email, SMS or suitable channels.
- ADP IT must establish suitable mechanisms to send notification alerts automatically to all ADP employees.
- Employees should not refer or forward virus warning till specified by Security team.

User Responsibilities:

- ADP Staff should ignore unexpected email attachments, even from colleagues or from suspicious or unknown source.
- ADP Staff s should not download any freeware or shareware without approval from ADP IT department.
- ADP Staff should not install direct internet access without the approval from ADP Information Security team.

PASSWORD SECURITY POLICY

Objective:

The objective of the password policy is to set up a standard for the creating and managing strong passwords including its protection.

Scope:

The scope of this policy together with associated procedures covers all the (IS)’s environments managed by ADP.

This policy applies to:

- ADP Employees, including System Administrators and End users.
- Employees of temporary employment agencies.
- Business partners, vendors and agents.

Passwords Policy:

- Passwords are an integral aspect of information security. It’s the first layer of protection for the user accounts. A weakly chosen password will result in the compromise of ADP’s applications and entire network.
- All users of ADP’s (IS)’s are responsible for securing and selecting their passwords.

Baseline Password Policy:

- All ADP’s (IS)’s have to have identification and authentication through pass-phrases, one-time passwords or similar password to permitting user access.
- Passwords must be considered as confidential and must not be revealed to anyone, except in accordance with ADP’s management of password procedure for protection of passwords.
- Users are liable and responsible for all actions, including transactions, communication on ADP’s (IS)’s, use of their ID’s and passwords.
- Screen saver password must be enabled by Users (if it’s not applied by group policy) on their own PC’s to prevent unauthorized access.
- Critical System passwords must be changed immediately, whenever the employee terminated or leaves ADP.

REFERENCES

[1] Dowd, P.W.; McHenry, J.T., "Network security: it's time to take it seriously," Computer, vol .31, no.9, pp.24- 28, Sep 1998

[2] "Security Overview," www.redhat.com/docs/manuals/enterprise/RHEL-4- Manual/security-guide/ch-sgs-ov.html.

[3] http://www.networkworld.com/news/2011/030311-security-roundup.html

[4] IT Governance – What is It and Why is It Important? By Doug Shuptar, Published on May 7, 2012

[5] Donald G; Mohnish P; Uday P; "Methodology for Network SecurityDesign",1990

[6] Marin, G.A. ; Florida Inst. of Technol., "Network security basics",Volume 3, Issue 6

[7] Rahul Telang; Wattal, S. "An Empirical Analysis of the Impact of Software Vulnerability Announcements on Firm Stock Price", Software Engineering, IEEE Transactions on, 557 Volume: 33, Issue: 8, Aug. 2007

[8] Chess, B.; Arkin, B. "Software Security in Practice", Security & Privacy, IEEE, On page(s): 89 - 92 Volume: 9, Issue: 2, March-April 2011

[9] Schneier, Bruce. Applied Cryptography Protocols, Algorithms, and Source Code in C, Second Edition. New York: Wiley, 1995. Print.

[10] Pfleeger, Charles P., and Shari L. Pfleeger. Security in Computing. 4th ed. New Jersey: Prentice Hall, 2006. Print. 0-13-239077-9.

[11] Ciampa, Mark D. "Introduction to Security." Security Guide to Network Security Fundamentals. Boston, MA.: Course Technology/ Cengage Learning, 2009. N. pag. Print.

[12] "Abu Dhabi Police Structure." Abu Dhabi Police GHQ. UAE Government, n.d. Web. 21 Nov. 2013.