International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

The Network Security Policies of Telecommunication Industries in Sudan

Mohammed Ibrahim M. Gali[1], Dr. Abdelrahman Elsharif Karrar[2]

[1]Dor Al-Uloom Schools, Hofuf , Saudi Arabia

[2]Taibah University, Al Madinah Al Monawarah

Abstract: ***As networks grow and evolve, the risk of coming under attack increases. To help counter this threat, Cisco has developed the Cisco Self-Defending Network (SDN) strategy. To effectively implement this strategy an organization can leverage their comprehensive security policies. To implement an effective security policy, you must understand why a network security policy is required, common attack-mitigation techniques, the parameters of a secure network life cycle model, and in the end, how to develop a comprehensive security policy. Security Policy. In the past, most closed off from public access, today's networks are more often than not "open," and they are now vulnerable to attacks from both the inside and the outside. In addition, as time has passed, hacker tools have become easily available, and the technical knowledge required to use such tools has decreased. This scenario creates quite a challenge for the e-business. A balance must be maintained between the need to open up a network to support the evolution of the business versus the need to protect business information. A network security policy is necessary for a number of reasons, including new laws that require certain levels of protection, an increase in terrorist activity, and the increased risk of being hacked.***

Keywords: Computer Networks, Security Policy, Telecommunication, Security Risk Control

1. Introduction

The Telecommunication Companies Network Security Policy provides the operational detail required for the successful implementation of a safe and efficient computer network environment for these Telecommunication Companies. These security policies were developed based on the understanding of the administrative needs of the companies and an evaluation of the existing technical configuration and requirements. These policies are meant to complement existing Industrial telecommunication companies system in Sudan, and policies relating to computer data network security

2. Problem

The research problem in the Network Security Policy Purpose of this stage is to perform a security assessment of the current environment including an analysis of the major business processes, operating functions, organizational units and information systems and a thorough evaluation of the configuration and design of the existing network and systems infrastructure and main servers

3. Objectives

1) Security assessment of the Telecommunication Industries in Sudan existing environment including an analysis of the major business processes, operating functions, organizational units and information systems (and major risks associated) and a thorough evaluation of the configuration and design of the existing network and systems infrastructure and main servers
2) Development of a security strategy encompassing security organization, security policy definition and security management process including recommendations on the methodology to be used for maintaining the security policy in a dynamically changing environment, as well as the related procedures, standards and controls for the effective roll out of the policy, and the approach in enhancing user awareness regarding security issues of Telecommunication Industries in Sudan.
3) Security architecture design including gap analysis based upon the results of the current state assessment and contrasted to the defined future state with a migration plan to meet policy requirements and further development of the organizational and technical security measures identified in the previous phase, including risk assessment of proposed policy and solution

4. The Research Hypotheses

1) Satisfied evaluation output dependent on the good implementation of the policy and strategies of networks.
2) The perfect insurance networks depends on network Security architecture design, organization, Security strategy and policy
3) Plans and polices help to develop secure networks and increase performance and control

5. Policies

1) Computer Registration in Network1

Computer must be registered with the telecommunication companies, Technical and Network Services. Registration information will include at a minimum the following items:

- Media Access Control (MAC) address of all network interface adapters in the computer.
- Full name of the primary user of the computer. In the case of computers used by multiple individuals, the name and contact information, including email, of the person who is directly responsible for the

Licensed Under Creative Commons Attribution CC BY

2) Administrative Access to all telecommunication companies:

Technical and Network Services will have administrative level access to all companies owned computers which are connected to the computer data network reserved for staff, and terminals. Technical and Network Services will only utilize this access to a computer under the following conditions:

- At the request of the primary user or administrator of the computer network.
- To apply operating system or software application updates or patches to the computer.
- To investigate any suspicious activity by a computer which could lead to network degradation, violate industrial companies policies, or violate local, state, or federal laws. Use of administrative access by Technical and Network Services to perform an investigation on a computer may only occur with prior approval by one of the

3) Centralized Computer Network Authentication

The telecommunication companies will maintain a centralized computer authentication system for computers. Departments will notify Technical and Network Services of changes to employment status of an employee so that user accounts can be changed or revoked as necessary. Technical and Network Services will maintain documented procedures for departments to notify them of personnel changes

4) Preset Configurations

All telecommunication companies networked computers will have their operating systems and network capable software applications preset with settings approved by the Manager of Technical and Network Services, or designate.

These settings will provide a minimum baseline configuration of computers that will ensure computer network security and integrity.

5) Authorized Servers Only

Technical and Network Services will maintain a list of all computers connected to the computer data network reserved for faculty, staff, and computer labs which are running any network service which is remotely accessible by another computer. Only computers which appear in this list are allowed to run the network services for which they are authorized. Network services must be approved by Technical and Network Services before they will be allowed to run on the company computer data network reserved for branches, staff, and terminals. Technical and Network Services will maintain documented procedures for network users to request to run network services on a computer which has not already been approved to run said service. If a previously approved network service on a computer has been found to cause network degradation, violate telecommunications companies policies, or violate local, state, or federal laws, the network service authorization for the computer will be revoked

6) Approved Computer Network Device List

Technical and Network Services will maintain a list of approved network devices which may be attached to the computer data network reserved for company, staff, and terminals.

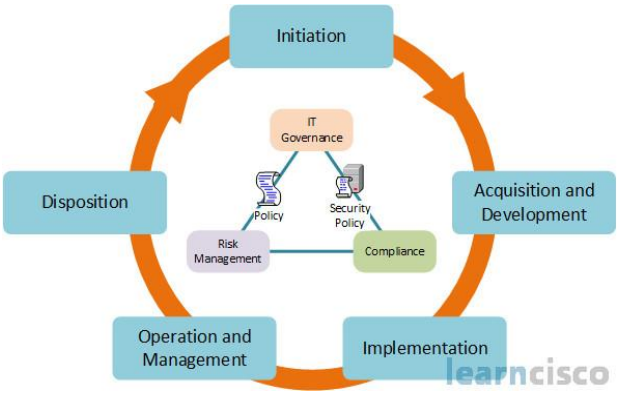

Figure1: Network Security Life Cycle

6. Policy Revision Process

1) Changing Environment

The industrial telecommunication companies, administrative, technical, policy, and legal environment of the telecommunication companies, as it relates to information technology use and security, is constantly changing. The Network Security Policies will be revised as needed to comply with changes in law or administrative rules or to enhance its effectiveness.

2) Change Drivers

A number of factors could result in the need or desire to change the Network Security Polices.

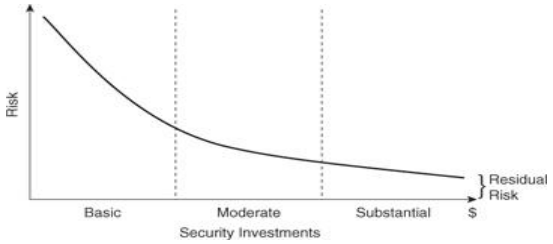

Figure 2: Security Investment: Diminishing Returns and Residual Risk

3) Change Process

- Updates to the Network Security Policies, which include establishing new policies, modifying existing policies, or removing policies, can result from three different processes:
- Every time new computer network technology is introduced into the company a security assessment must be completed. The result of the security assessment could necessitate changes to the Network Security Policies before the new technology is placed into use in the telecommunication companies computer network.
- Any user may propose the establishment, revision, or deletion of any policy at any time. These proposals should be directed to the Manager of Technical and Network Services or designate who will evaluate the
- propose and make recommendations to the managers if the proposal is deemed valid and reasonable in accordance with the goals of the Network Security Policy

4) Changing Environment

The industrial telecommunication companies, administrative, technical, policy, and legal environment of the

Licensed Under Creative Commons Attribution CC BY

telecommunication companies, as it relates to information technology use and security, is constantly changing. The Network Security Policies will be revised as needed to comply with changes in law or administrative rules or to enhance its effectiveness.

5) Change Distribution and Notification

The telecommunication companies Network Security Policies are likely to be impacted by changing technology, legislation, educational and administrative requirements. The steps for permitting and documenting an exception are:

- A request for an exception is received by the Manager of Technical and Network Services or designate along with a rationale for justifying the exception.
- The Manager of Technical and Network Services or designate analyzes the request and the rationale and determines if the exception should be accepted, denied, or if it requires more investigation
- If more investigation is required the Manager of Technical and Network Services or designate and telecommunication companies computer technical support staff determine if there is a cost effective solution to the problem
- that does not require an exception.
- If there is not an alternate cost effective solution, and the risk is minimal, the exception may be granted.
- Each exception must be re-examined according to its assigned schedule. The schedule can vary from 3 months to 12 months depending on the nature of the exception.

References

[1] Adams, C, Simple and Effective Key Scheduling for Symmetric Cipher,SAC,2004.
[2] Alvare, A, How Crakers Crack Passwords to Avoid, Proceedings, Security Workshop II, August 2000.
[3] Anderson, J, Computer Security Threat Monitoring and Surveillance, P.Anderson Co, 2002.
[4] Alexander, S, Password Protection for Modern Applications, login, 2004.
[5] Andrews, M., and Whittaker, J, Computer Security IEEE security and Privacy, 2004.
[6] A. Bonnaccorsi, “On the Relationship between Firm Size and Export Intensity,” Journal of International Business Studies, XXIII(4),pp. 605-635, 1992. (journal style)
[7] R. Caves, Multinational Enterprise and Economic Analysis, Cambridge University Press, Cambridge, 1982. (book style)
[8] M. Clerc, “The Swarm and the Queen: Towards a Deterministic and Adaptive Particle Swarm Optimization,” In Proceedings of the IEEE Congress on Evolutionary Computation (CEC), pp. 1951-1957, 1999. (conference style)
[9] H.H. Crokell, “Specialization and International Competitiveness,” in Managing the Multinational Subsidiary, H. Etemad and L. S, Sulude (eds.), Croom-Helm, London, 1986. (book chapter style)
[10] K. Deb, S. Agrawal, A. Pratab, T. Meyarivan,“A Fast Elitist Non-dominated Sorting Genetic Algorithms for Multiobjective Optimization: NSGA II,” KanGAL report 200001, Indian Institute of Technology, Kanpur, India, 2000. (technical report style)
[11] J. Geralds, "Sega Ends Production of Dreamcast," vnunet.com, para. 2, Jan. 31, 2001. [Online]. Available: http://nl1.vnunet.com/news/1116995. [Accessed: Sept. 12, 2004].(General Internet site).

Author Profile

Mohammed I. M. Gali the B. Sc in Computer Engineering, Faculty of Electronics Engineering, Beni-Walid University , Libya 1992 and M.Sc. degrees in MSc. Computer Science, The National Ribat University, Sudan, 2012

Dr. Abdelrahman Elsharif Karrar PhD, M.Sc. and B.Sc. in Computer Science. He is Associate Professor College of Computer Science and Engineering Taibah University – Saudi Arabia

Licensed Under Creative Commons Attribution CC BY