UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

SCIENTIFIC REPORT

THEME:

"MANAGEMENT SYSTEM FOR PERIMETER SECURITY AND ACCESS DISTRIBUTION NETWORK OF THE SAVING AND CREDITS COOPERATIVE ESSENCE INDIGENOUS LTDA. IBARRA, BASED ON THE ISO 27002:2013 NORM"

AUTHOR: KARINA ESTEFANIA QUILCA BURGOS

DIRECTOR: ING. DIEGO TREJO

IBARRA, ECUADOR

2016

"Management system of perimeter security for access and distribution network of the Saving and Credits Cooperative Escencia Indígena Ltda. Ibarra, based on the ISO 27002:2013 norm" (April 2016)

Author: Quilca, K. karo Keqb2890@hotmail.com
Director: MGS. Trejo D. Djtrejo@utn.edu.ec

Summary- *this project presents a management system of perimeter security for access and distribution network of the Saving and Credits Cooperative Escencia Indígena Ltda. Ibarra, based on the ISO 27002:2013 norm. The same that consists of a manual of policies and good security practices directed to all officials of the company, the deployment of a firewall, IDS/IPS and a demilitarized zone (DMZ), which was achieved thanks to the deployment and configuration of a equipment of UTM technology gateprotect 500 with GPA.*

Index Terms **-**DMZ, IDS/IPS, UTM

I. INTRODUCTION

The savings and credit cooperative Escencia Indígena is a financial company of private character created by a group of enterprising people of the province of Imbabura and Tungurahua on 19 May 2007. Has a group of servers (database, Mobile window, facilitated, APP windows, intranet, etc. Located in the Agency Ibarra which serves as an array and from there are distributed and controlling services and applications to the rest of the agencies located in various cities of the country. (Castañeda, 2013b)

II. ANALYSIS OF THE CURRENT SITUATION

At present there are different methodologies for the analysis of information security risks of a public or private entity. In view of the fact that in the ISO/IEC 27002:2013 is not specifies a methodology; for this study was selected the OSSTMM methodology (Manual of the methodology open security testing) due to the advantages that it offers.

This methodology encompasses all the security operations are based in different areas or channels as described by the manual, and is shown in Figure 1:

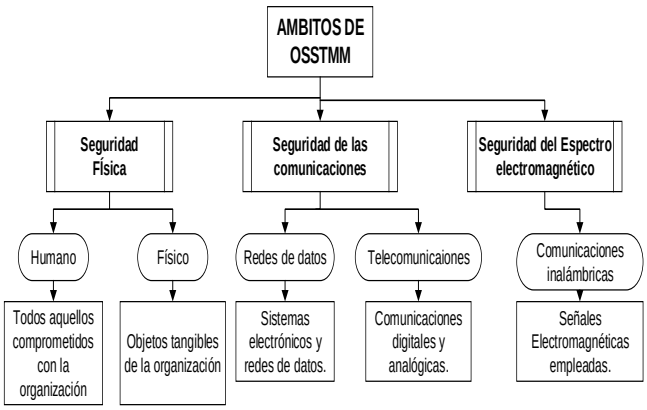

Figure 1: Areas of OSSTMM
Source: (Valdez Alvarado, 2013)

The simplest way to make RAVs is to use the worksheets created specifically to calculate the area of attack and multiple metrics required from the test data. This worksheet is available on the web site of ISECOM. The analyst need only enter the values in the white boxes empty, and the rest of the calculations are handled automatically (Herzog, 2003).

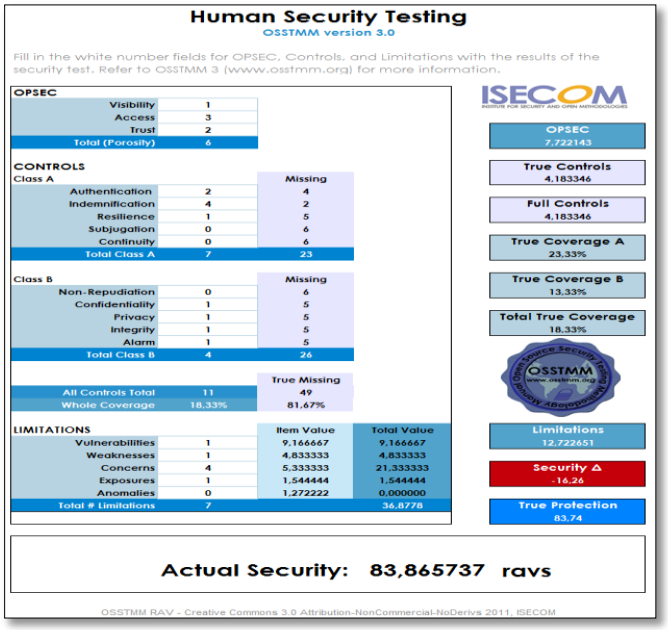

Figure 2: Calculation of the RAVS in Human Channel.
Source: Obtained from RAVs OSSTMM Calculator 3.0

A. Human Channel

The safety analysis in this channel, was carried out at the level of access and trust that this delivery to the security of the information. For which it conducted tests for direct observation and social engineering, with what was achieved very valuable information which compromises the security of the information of the company.

The obtained result reflects according to the parameters of the methodology that safety is considerably low, reflected in the lack of manuals of standards and good practices of the correct use of the information currently implemented by the administration.

It has a high degree of priority with regard to the compensation of personnel, but not in other controls that are totally nulls as the subjugation and Continuity.

B. Physical Channel

The safety assessment on the physical channel, was focused on the level of access to the room of equipment, the availability of devices and especially to the response to eventualities of the same.

To perform the test of physical security and analyze existing controls was determined which unfortunately does not have implemented some physical security controls the same that are a perfect target for attackers to computing.

C. Telecommunications Channel

The safety assessment on this channel, was a port scan, with the help of software Zenmap, leaving in evidence the level of access you have to applications.

The results obtained are reflected according to the parameters of the methodology and determined that you have only controls of compensation, authentication and privacy; the other controls are zero; opening a gap for the insecurity of the information.

The limitations are valued individually but are related with some controls and operational safety, because the values in operational safety are high, the calculation of the limitations is too. Therefore highlighted limitations as vulnerabilities, weaknesses and exhibits the same that reflect an administration not suitable exposing the network to certain computer threats.

D. Data Channel

Aims to monitor the input and output data of the communications network via the web, instant messaging, chat, forums of discussion based on the Web, or by e-mail, with the purpose of verifying if I bring malicious codes, inappropriate behavior.

The results obtained are reflected according to the parameters of the methodology and determined that the operational safety is very high, mainly in the aspect of confidence, in which it has been considered all ports that are open. This reflects the importance that has been given to the security of telecommunications

According to the test, it was noted that there are only controls of compensation, authentication and privacy; meanwhile the other controls are zero; giving rise to insecurity of the information.

III. DESIGN AND IMPLEMENTATION OF THE PERIMETER SECURITY SYSTEM

Was designed the system of security both to access level and at the level of distribution. To access level is raised awareness to users and administrators of the assets of the company through the creation of a manual of security policies based on the controls of the ISO/IEC 27002 norm. At the level of

distribution is implemented a computer gateprotect GPA 500 which performs the functions of firewall, IDS/IPS also permitted the configuration of a demilitarized zone.

A. Security Policies

Once identified the risks of security, controls were selected to ensure its reduction to an acceptable level; taking into account that no set of controls can achieve the complete security. It is proposed to create a guide of policies and good practices with the aim to improve the management of information security, as well as sensitize officials and administrators of information assets in the proper use of the same.

The manual of policies and good security practice was based on the Standard NTE INEN-ISO/IEC 27002:3013; the same that establishes guidelines and general principles to initiate, implement, maintain and improve the management of information security in an organization. The objectives set out in this standard provide a general guide on the commonly accepted goals for managing the security of the information.

The selected domains were:

1. Security Policies
2. Organizational aspects of the security of the information.
3. Security linked to human resources.
4. Asset Management
5. Access Control
6. Encryption
7. Physical and Environmental Security
8. Security in the operative
9. Providing telecommunications security
10. Acquisition, development and maintenance of information systems
11. Relations with suppliers
12. Management of Information Security Incidents
13. Security aspects of the information in the management of business continuity
14. Compliance

B. Topology

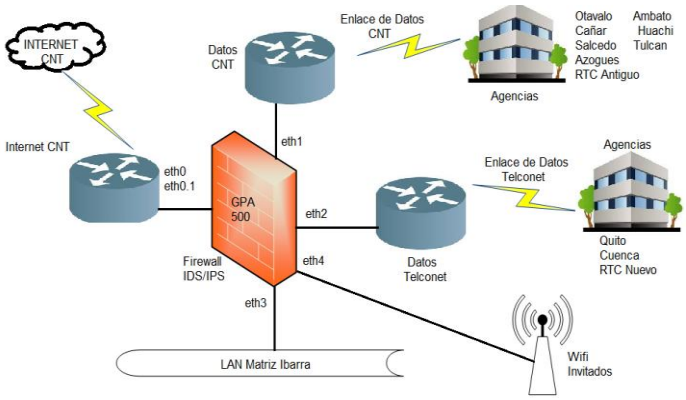

Figure 3: Design of Perimeter Security.
Source: Development of the project

Security threats are every day more complex and dangerous, moreover, are causing losses and high costs for the companies. The products that integrate effective solutions against these threats are systems whose operation is difficult to understand and administer and requires too much time and attention on the part of those responsible for it, which becomes a problem given the steady increase in the work of that department. This inevitably increases the possibility and the risk of errors on the part of users, configuration errors and operation in the systems, errors that currently represent more than 90% of the vulnerabilities and gaps in the perimeter security at companies.

It was not considered eligible by a solution by free software due to the work load that has the systems area. Due to a solution by free software does not provide the integration of services and their administration, monitoring and maintenance is more complicated because in most cases has to be performed via console and use processes more complicated and involving more time to identify failures and errors in the system.

TABLE 1
SOLUTION COMPARISON

Feature	Gateprotect GPA 500	Free Software
GbE Ports	It has 6 ports	You need at least 3 Network cards
Benefits	Firewall, DMZ, IDP/ips, virus filter, web filtering, spam detection, IPSec/SSL, VLANs, VPN, QoS, load balancing.	Requires configuring servers separately
Firewall performance (MBit/s)	2100	Operating system dependent
Exposure to vulnerabilities	Very small	Own the operating system and incorrect configurations.
Costs	By licensing with included support.	Cost of learning, installation, migration, of interoperability.
Mode of Operation	Friendly with the user or administrator	Complex

Source: Project Development

C. Perimeter Solution

As a first step to perform is the installation of the firmware of the computer firewall to allow access to all the benefits that this equipment offers.

Subsequently enters all the objects that make up the network of the company with their respective configurations and gets a topology as shown in Figure 4. This is divided into two areas:

The first (left) allows access to networks of agencies and suppliers of services such as: database server connected through a VPN to the server Fitbank, is also the VPN between the LAN (Ibarra) and the server connects and wifi is connected with the other area.

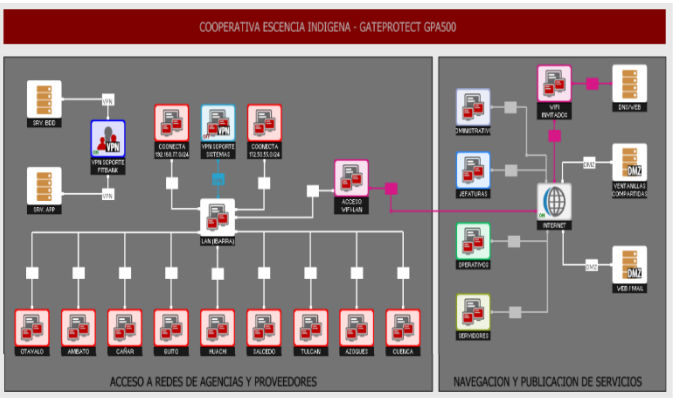

Figure 4: Network diagram of the company.
Source: Administrator obtained GPA500

The second area allows navigation and publishing services. This area contains the following objects: servers (own of the company), chiefdoms, operators, DMZ, Wifi guests.

For the DMZ have considered the web servers, email and Windows Server.

To configure the IDS/IPS Firewall gateprotect uses profiles. Each profile can be adjusted and assigned to a network interface. The rules of a profile can be adjusted to different states.

The IPS provides 5 different states, DISABLE, log, DROP, DROP_LOG AND REJECT to configure rules individually, the IDS has two different states, LOG and DISABLE. States define the traffic that is lateen with the rules

The IDS/IPS only produces reports of alarm if are recorded attacks in the IP addresses of a particular group of computers.

The intrusion detection system monitors special computer systems or networks, e.g. a network server, a mail server or a DMZ in particular.

IV. OPERATION TESTS

1. Statistics of locks

On the toolbar you can use the toolbar in the Customer Statistics for:

Print the statistics, change the language of Customer Statistics for menu and use, obtain information on customer statistics, End Customer Statistics.

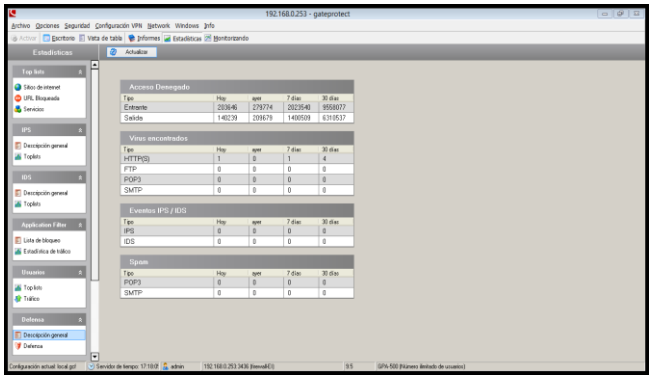

Figure 5: Statistics of locks.
Source: Administrator obtained GPA500

You can filter the results displayed depending on the statistical information prepared at the top of the

statistics window:

Desktop: complete network, users or computers

Period: 6, 12 or 24 hours or 7 or 14 days, 1, 3 or 12 Months

Period of self-definition with date and time for the start and end

Time Window: Any time of day with start and end

Access blocked: Entry or Exit

2. Attempt to access locked page, Access Denied correctly.

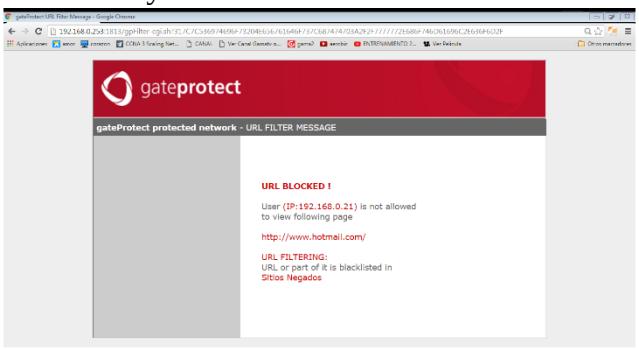

Figure 6: Access denied.
Source: Administrator obtained GPA500

V. COST ANALYSIS

A. Cost of equipment

At this point is detailed the value of the equipment necessary for the implementation of this design described in Table 2. The analysis was based, in the equipment available in the national market, the popular brands and prices references the same.

Table 2
Cost of equipment

Equipment Costs			
Equipment	Quantity	Price	
		Unit Cost	SUBTOTAL
GATEPROTECT GPA 500	1	$ 4.032,00	$ 4.032,00
Client PC	1	$ 300.00	$ 300,00
TOTAL			**$ 4.332,00**

Source: Proforma company SMART HELP SOLUTIONS

B. Engineering Costs

In the engineering costs is considered the cost of installation service and computer configuration shown in Table 3.

TABLE 3
ENGINEERING COST

Engineering Costs			
Equipment	Quantity	Price	
		Unit Cost	SUBTOTAL
Security System Design	1	$ 400,00	$ 400,00
Installation and Configuration	1	$ 100,00	$ 100,00
TOTAL			**$ 500,00**

Source: Proforma company SMART HELP SOLUTIONS

C. Total cost of the security system

TABLA 4
TOTAL COST

Total costs of security			
Description	Unit	Qty	TOTAL
Equipment	U	1	$4.332,00
Engineering	U	1	$ 500,00
TOTAL			**$4.832,00**

Source: Project Development

The implementation of this project has a value 4032 dollars due to the PC for the administration already had the company and the value of engineering was part of the development of the project.

The benefit to the company in addition to the already mentioned is that when you buy this solution is that to opt for this solution and have opted for separate servers are these of free software it was necessary to hire a person in charge of the perimeter security servers because the load for the systems department is too far. With this to hire an employee with a minimum salary of $600 in the 12 months that lasts the license on your computer would be an investment of 7200 dollars exposing themselves to faults because the systems are not as robust as is the settlement of gateprotect. With the raised solution is secure the technological infrastructure of the company and increases your productivity based on

three key points: reduction of time, error reduction and reduction of costs.

VI. Conclusions

Know the technological infrastructure of the company and the interviews with the administrator of the technological infrastructure of the company was the first step to develop the project since this allowed to know the risks and weaknesses.

The ISO/IEC 27002:2013 does not establish a methodology for risk analysis and risk management software, but recommends choosing a methodology that most relate to the needs and characteristics of the entity to analyze.

The risk analysis was carried out on the basis of the channels and parameters described in the manual of the open methodology of testing of security (OSSTMM), by which it was determined the level of risk to which it was exposed the company.

The risk analysis made in the COAC "Essence Indigenous" allowed mitigate and eliminate or transferring the risk of the failures that affected the performance of the network; among which it was able to highlight the insecurity and poor state of its fourth of computers.

The manual of information security policies is the most important document in which is based the decision-making and action to be taken on security issues, no internal legislation or procedure is on the policy and any violation of the same shall be punished according to the internal rules considering the analysis that if the damage is very serious steps should be taken severe.

Housed the web servers and mail in a demilitarized zone DMZ in order to allow connections from both the internal network and the external, while connections that depart from the DMZ are only possible with the local network.

The computer gateProtect 500 integrates multiple security services as is: firewall, DMZ, IDS/IPS in addition to control spam, antivirus, proxy and other which makes it a comprehensive solution at the time of protecting a network.

Using the cost analysis it was determined that use the computer gateprotect GPA 500 is the most convenient way to ensure the stability and continuity of the business; because this computer provides the best features as assurance of perimeter networks.

After making the comparison between a solution with free software and the computer GPA 500 it was noted that it has a greater cost savings in relation to the training, installation and administration that requires the solution by free software.

To implement this solution the company will have greater stability and control of your network; i.e. there will no longer be so much congestion and loss of connection so that the attention to their customers or partners will be quicker and more efficient than earlier which represents an increase in their productivity and business development.

References

[1] Dictionary of Computing and Technology. (2015*). Dictionary of Computing and Technology*. *Obtained from Definition of brute force:* http://www.alegsa.com.ar/Dic/fuerza%20bruta.php .

[2] Castaneda, D. (2013). *Indigenous Essence*

[3] Erb, M. (2009). *Risk Management on computer security. Obtained from* https://protejete.wordpress.com/gdr_principal/definicion_si/.

[4] Garcia, A., Hurtado, C., & Alegre, M. (2011). *Computer security. Madrid, Spain: Auditorium*.

[5] Pebble, Á. P. (2012). *Perimeter Security*. *Obtained from Https://alvaroprimoguijarro.files.wordpress.com/2012/01/ud03_sad_alvaroprimoguijarro.pdf.*

[6] Herzog, P. (2003). *OSSTMM 2.1*.

[7] Herzog, P. (2003). *OSSTMM 3.0*.

[8] INEN NTE-ISO/IEC 27002. (2009). *Information technology - Security techniques - Code of Practice for the management of information security. Quito.*

[9] Superintendence of Popular and Solidarity Economy. (2012). *Regulation to the organic law of the popular and solidarity economy*.

[10] Toth, G., & Sznek, J. (2014). Implementation of the NIST SP800-30 guide through the use of OSSTMM. Neuquén.

[11] Valdez Alvarado, A. (2013). OSSTMM3. Analysis and Design of Information Systems.

Bibliography

Karina Estefanía Quilca Burgos

She was born in Ibarra on 28 May 1990. She completed his secondary studies at the Technical College "Victor Manuel Guzman", there she obtained a degree in Informatics.
In 2008 she joined the Universidad Técnica del Norte, she is a student of pre-grade in the career of Electronic Engineering and Communication Networks.