RISK MANAGEMENT REPORT

Contents

Executive Summary

Introduction

Purpose

This document represent an assessment of the security network of the Silicon Craft Company. Encompasses an evaluation of the existing network threats and the proposed security measures to be taken by Silicon Craft Company.

Scope

The scope of the report is basically to perform a deep security assessment of the network and checking the penetration testing through the public access and internet access of information of the Silicon Craft Company.

The Silicon Craft Company has the following Internet Protocol addresses (IP address)

168.254.0.15-27 and 168.254.0.1-7

The following are workers that will be subjected to social engineering assessment

Kevin Morgan, Thomas Samson and Duke Douche.

Another critical assessment that is going to be done is on the performance of a web application penetration. The following domains will be put into consideration.

http://www.siliconcraft.com

www.siliconcraft/employees.com

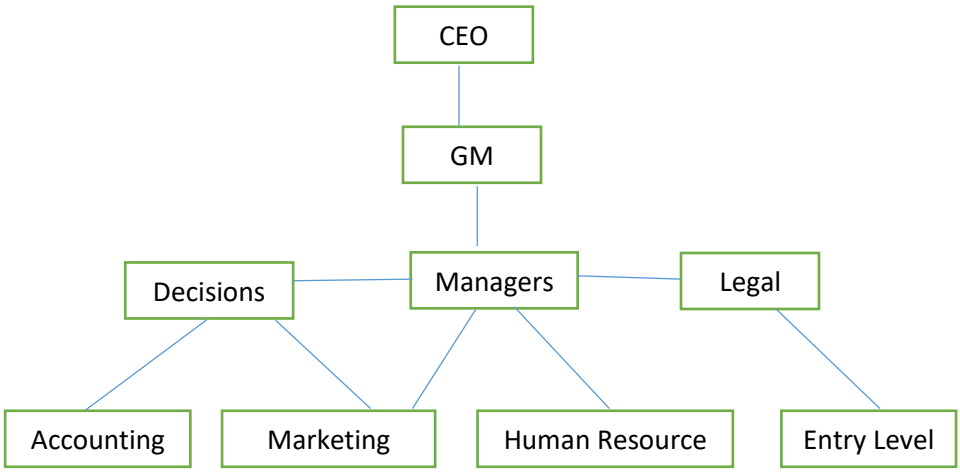
Organization Network Overview

Organization's Mission

The mission of Silicon Craft Company is provision of access to individual records for both the individual themselves and the organization at hand who created the records, without interfering or compromising the identity of that individual. Either by exposing their data to an unauthorized personnel.

Organization Structure

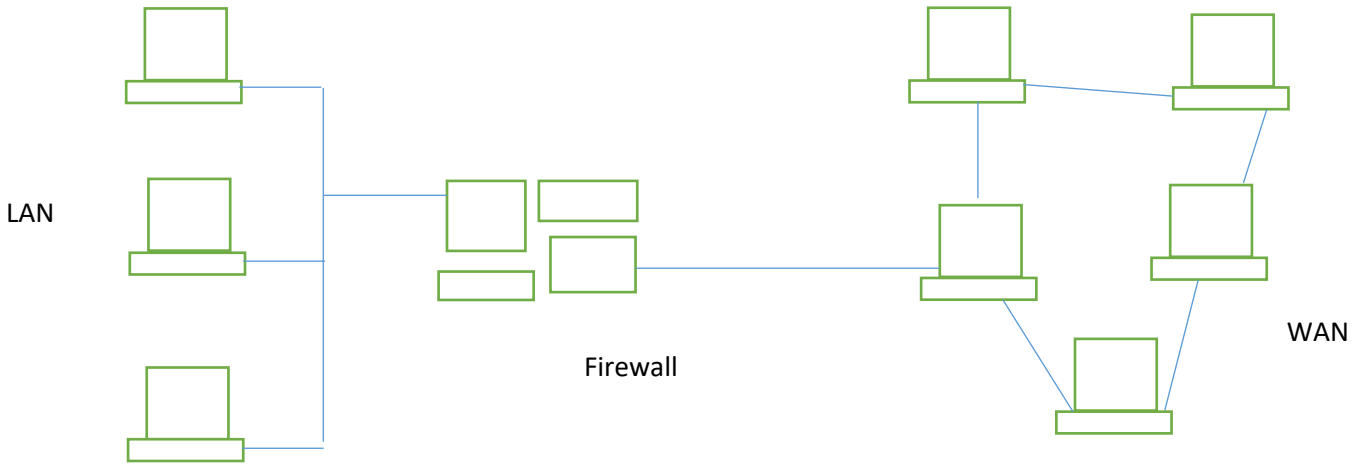
The chart below shows the structural organization of the Silicon Craft Company. Starting from the Chief Executive officer, all the way to the entry level. This is where individual data is being entered into the databases of the organization at large. It has department levels and each department has a manager. The manager assigns employees within that department different tasks that when combined, brings about the normal operation of the company.



Network System Description
Diagram of the Organization (LAN, WAN, Intranet, extranet, internet)

The diagram below shows how local area network and wide area network works in the silicon craft organization. For the Local area network, these are computers that are connected within a department of Silicon Craft. For example in the financial department. Information is being shared among the employees within that department.

For the Wide area network, this is where information is being shared at large by the whole organization. Departments sharing information and sending to the servers for backups and for easy access to them by any authorized members.



System boundaries
This is important since it controls the flow of information within and outside the network and prevents access by unauthorized personnel. System boundary protection will check on the physical security, least functional devices, default denials, configuration of changes and documentation, monitoring of firewalls and logs, detection of malicious code, security updates and finally periodic reviews.

Security updates- this will be done on annual updates. And by this providing up to date information about their vulnerabilities and apply relevant patches, updates and other recommended protection actions.

Periodic review- after the configurations of firewall, reviews will be made on at least annual basis. This will be done to ensure that the whole system is compliant with the procedure of updates and service support.

Firewall monitoring and logs- the system boundaries protection devices shall be monitored on occasional basis for any suspicious activity and inappropriate use of devices. Finally firewall logging capability shall be utilized just as per the proactive monitor procedures.

Vulnerability Assessment Methodology
Network is like the main stream of a business. Network is what keeps information of the organization flowing and it also makes sure that the daily operation of an organization goes on well without any interruption. A good network system that has been set up well and all the vulnerabilities put into consideration helps an organization to boost its daily operation and this maximizes job output and increasing profits of the organization at large.

In order to ensure that the objective of the organization is met, network is supposed to be made secure and that should be done on regular basis. Either annually or weekly. Depending on how data is important to the organization and those using it.

The method that the team is going use to test the vulnerability of the network of Silicon organization is

1. Check whether there are open ports
2. Checking if there are unpatched software or applications install.
3. Doing a full network scan of all the devices connected in the network.

The team will use vulnerability scanner. This scanner is important in that it will identify open ports, IP addresses in use and the operating systems and application that are being used in the organization.

The scanner will the compare what it has recorded with the main databases in the organization and give a concrete report on the finding. Based on vulnerability.

This will be presented based on the risks. From high to low.

After this, the team will be able to identify if the vulnerabilities found are very dangerous to the organization at large, or whether the findings are false, of even if the ports that were left open were done so intentionally.

And by this, the team will come up with the findings if the assessment done could lead to potential risk to the organization from each discovered vulnerability, and the chances of these vulnerabilities being used as an attack loop holes to the organization.

If the vulnerability will be a loop hole to the attack of the organization, the team will come up with the most appropriate rules and procedures to fix them. Some will be done by patching applications and software, but others will need more in-depth and time to fix.

Another method that the team will use to test the vulnerability of the network is through penetration testing. This is method is vital in that it checks the existing vulnerabilities are exploited to see how much threat they can be to the network. It also looks at how much the attack could damage the organization system in case the attacker uses a certain vulnerability.

By this, the team will ensure that vulnerability testing targets both the network within the organization and outside the organization. This will ensure that the silicon Craft gets an indication of the potential threats that are around or outside that an attacker could look to exploit.

Network concepts

TCP/IP model

TCP/IP gives rules and procedures on how data is exchanged over the network by providing end to end communications tat identify how it should be broken into packets, addressed, transmitted, routed and received at the destination. TCP/IP being managed by system administrator with the capability of recovering automatically from the failure of any device on the network.

How it works; it uses the client/server model of communication. Here a user which is the client machine id provided a webpage or service by a server in the network.

Each client's request is put into consideration as new request because it is unrelated to the previous request.

It transmits a single message, and remains connected until all the packets n a message have been sent to the required destination.

TCP/IP model has four layers; application layer, transport layer, network layer, physical layer.

The TCP/IP model of the Silicon craft organization is highly scalable and as a routable protocol it determines the most efficient path through the network.

Firewall

Firewall is a software or a hardware within a network system. Its role is to protect the network of computers from being attacked over the internet either by hackers, viruses or even worms.

The attacks may take place either at LAN level or WAN level within the organization.

Having a firewall in Silicon Craft organization, it will allow in the setup of some business rules such as control of access to certain sites, and giving clear regulations on how employees will be using the network.

Firewall controls activities done online through the following ways;

- Packet filtering-in that, small amount of information is checked or analyzed and then distributed accordingly.
- Stateful- here inspection is done to match specific details of a data to the database of the information
- Proxy service-here, the firewall saves online data and it sends the data as per the requesting systems during job operation. (The importance of having firewall, n.d.)

Network Monitoring Tools

Network monitoring is necessary for Silicon Craft Firm. The whole purpose is to monitor, check computer network usage and performance, and also check for slow or failing of the whole system.

After the check, the system will notify network administrator of any performance issues. This is important because the system will save a lot of money and reduce many problems that might face Silicon craft at large. It is important since it is the best way to ensure that daily activities within Silicon Craft is moving on smoothly.

Some of the advantages of network monitoring will be:

1. Security- information within the organization needs to be kept secure. Network monitoring will always keep records or tracks of all activities and alert the network administrator of any slight issues that can be handled quickly before they become real big issues. Some of the things that network monitoring can alert is, if something stops responding suddenly, or if storage capacity is low, or even during failure of servers. It will helpful since monitoring will be done throughout 24/7
2. Troubleshooting- there is also another important and advantage of network monitoring. This is none other than troubleshooting. It saves a lot of time when you try to diagnose what is wrong within the organization network. With network monitoring, the system administrator will be able to tell which device is actually bringing problems within the whole network system. Hence being able to send support team to work on a problem and before it is known, it should be fixed as soon as possible. When problems are left to escalate, or get even bigger, it might be very difficult to narrow them down or even get them fixed. But through network monitoring, this will be of great help to understand what is really going on. And how to come about fixing the issue.
3. Saves Time and money- network monitoring will save the Silicon Craft a lot of money and time. Without network monitoring, a lot of time would be spent checking the network and this might lead to more hours having to be worked on. Some of the negative effect that will face the organization is poor or low productivity. Network monitoring is important since when you can identify a problem and fix it as soon as it can be fixed, the Silicon Craft organization increases its performance hence profits gained. And when everything is running smooth, a lot of time is given for the organization to run its business. Through network monitoring, the system administrator is able to understand all devices that are being used within the network, and also be able to identify what needs additional disk space.
4. Plan for change- network monitoring enables system administrator to track if there is a device within the organization that is running near its limit or needs to be changed Network Monitoring also gives you the ability to plan ahead and easily be able to make the necessary adjustments. (itnow, n.d.)

Wireshark and Nmap- these are tools used to capture network packet when an attacker to a network is scanning target using nmpa port scan method. The wireshark and nmap installed in the network captures different network traffic packet for open and close ports.

Os Monitoring Tools

Checking out the performance of operating systems and processes is important to debug processes and systems for effective management

The main tool that the team agreed to be installed and used as an OS monitoring tools is the PRTG tool.

This is because,

- It is compatible with all the most popular operating systems.
- It has custom monitoring sensors which allows you to synchronize and monitoring network with the user's application ideas.
- It is easy to configure.
- It balances monitoring for distributed and load balancing.

OpenVAS/ MBSA – these are frameworks for offering services in managing vulnerability solution. The team agreed that they be put as a measure in the network. In that they will help

Database Concepts

Silicon Craft company produce and gather data as it operated. In their database, data is typically organized in a way that is relevant to the model and it supports processes requiring the information. Being able to understand how this can be able to be managed effectively is essential in Silicon Craft Company.

The company employs Database Management System (DBMS) to help them in effectively management of their data and derive relevant information out of it. The system supports data management directly. It is a package that is created to define, manipulate and manage data stored within a given database in the organization.

It is essential because of the following reasons and their importance:

1. It allows definition, creating, querying, updating of databases
2. It define rules to validate the data and relieve users of framing programs for data maintenance
3. It changes the existing database
4. It creates rules for business applications.

For the access controls of the database, this is important in that;

1. It ensures security by preventing or detecting unappropriated information
2. It ensures there is integrity, this is by preventing and deterring improper change of information within the database.
3. By ensuring system availability- this is by preventing improper denial of service that database management systems offers.

Findings

After a comprehensive assessment of the Silicon Craft network, we identified the following information concerning the security and its strength.

1. Due to network exposure, the network infrastructure portrayed most configuration be having a concrete effort in minimizing risks and providing limit access to the services.
2. Due to network user's credentials, the control of how users access information was very strong in that it was very difficult to find or get a set of user names and password even after trying using many methods of penetrations. This indicated that the organization had really put in place a very high value protection on sensitive data of individuals

For the finding, this was a positive thing to the team. And therefore encouraging the maintenance of the system.

Network-related

Os- related

The team found the following conclusion based on the analysis of MBSA's reported vulnerabilities. In the when MBSA is used to scan one of the servers, it come back saying that four critical updates couldn't be verified or the servers needed some updates. In most instances, this is because windows updates majorly focused on OS updates, whereas MBSA is also trying to check for application-level vulnerabilities.

Identity Mgmt.

1. For the network vulnerabilities- the team identified the following network vulnerabilities.
    - There was firewall TCP rule bypass. There was an issue with firewall on how it handled specifically crafted TCP packets. On the first IP address provided, firewall monitored the packet that was being received and checks whether there was an existing established connection. If it was a 3 way handshake, it was verified that a rule allowed access and then processed the transferred packets accordingly. The problem with this came about when there was FIN or RST flags on the initial packet of 3 way handshake. At the end this created a n unusual combination of flags. Bypassing the firewall rule came about when the estimation server process the packet as a 3 way handshake initiator.
    - Open ports that were identified to be open were 443(http), 25(smtp), 80(http public site), 21(ftp)
2. For the web application vulnerabilities, there was sql injections. In that an sql injection vulnerability was discovered on the employee.com page which allowed collection of employee detailed and updating existing tables.
3. There was information disclosure. This was as a result of the network providing error message indicating an invalid details not found. This information was discovered that it could be used with social engineering type of an attack for someone to gain access to client's details or sensitive information.

Recommendations

Due to the advancement of technology, network monitoring tools are being launched daily. Going through all the network monitoring tools, the team was able to highlight their main strengths and why the team thought they are in the top class of tools to be used by the

organization. This was done considering some of the feature are like uptime/downtime indicators, efficiency through alerting systems to the administrator via sms or emails.

Some of the tools that the team recommended:

1. Installation of Solarwinds Network performance Monitor. This is because, it is easy to setup, the tool automatically checks and discovers network devices within the network and deploys them within a few minutes.
    - It product can be customized and also its interface is easy to change and manage.
    - It was also noted that solarwind support for wider array of OEM vendors, it has a great forecast and capacity plan.
    - It is quick in pinpointing out problems or issues with Network performance and critical path visual features.
    - It has dashboard that can be used to analyze critical data points and paths across the network.
    - It has a robust alerting system with options to simple and complex triggers.
2. Paessler PRTG- this is also among the network monitoring tools that the team suggested to be installed in the network system. This tool is known because of its advanced infrastructure management capabilities. In that all the devices, traffics of the system, and also applications within the network can be displayed easily in order to view the performance summarized and alerts.
   Paessler networking tool monitors the whole system using technologies like SNMP, REST API, WMI, Sql, SSH
   Another interesting feature about Parssler PRTG is that its ability to monitor network devices within the datacenter using a mobile app. In that there is a QR code that relates to the sensors and once printed out, it's being attached to the physical hardware, the mobile app is then used to scan the code and all information about the device is displayed on the mobile screen.

Risk Management

Accepting Risk- this is the type of risk that happens when a company accepts that the potential loss from a risk is not huge enough to warrant or spending money to prevent it from happening. (Accepting risk, n.d.)

Transferring Risk- it is a risk that exists when there is more than one party involved. This will be written down into a project contract.

Mitigating Risk- here the team limits the impact of the risks identified. So that if the risk occurs, the problem is created in small manageable and easy to fix.

Eliminating Risk- this can be done by changing the plan completely to avoid the risk from having a large impact on the organization.

Risk assessment Results.

Risk	Likelihood	Impact	Main Cause	Mitigation
Contractor failure	medium	High	In some scenarios, a contractor may fail to deliver a desired product in time. As a result, a new process of sourcing another contractor needs to be initiated resulting into significant loss of time.	To curb such situation, it is essential a contractor with adequate capacity be contracted
Optimistic schedules	Medium	High	Optimistic schedules are ones developed without proper analysis of the activities involved in each phase resulting into more time taken to complete a project	It is important that realistic schedules be developed with major emphasis laid on proper analysis of all the activities involved in each phase.
Disagreement with customer	High	High	Situation where, during user testing phase, the users (customers) differ with the developers especially in terms of the system functionalities or insist on new requirements. As a result, developers may	Friction with customer can be minimized by involving them right from the initial stage of project development

			have to construct other software code that meets the desired functional features	
Research-oriented development	Medium	Medium	This approach requires studying, analyzing and developing projects based on information gathered from other developers or researchers.	To avoid lateness, it is necessary that deadlines be properly adhered to during the development time.
Product is larger than estimated	High	Medium	If the estimated size of a product is much smaller than its real size, then the project development will take more time to complete than scheduled earlier. A project is measured by the different functions that it is supposed to deliver to its users.	To get a proper estimate of the product size, it is essential that metrics such as the Lines of Code (LOC) and Function Points are implemented
Incomplete Decisions	High	High	Incomplete decisions could lead to delays in deadlines for all assigned tasks	Making well rounded logical decisions without bias would ensure that the project requirements are met on time.
Lack of communication	High	High	Communication is the key to	keeping group members

			successful project completion	informed of any events that could affect the progress of the project
Insufficient Division of Labor	High	High	It's entirely possible that we lean too heavily on the skills of one individual or another.	As a small team, we should be aware of who has what skills to best utilize our available time, but we also need to make sure that one person doesn't become such a lynchpin that the project cannot continue without them should something happen to them.
Lateness	High	Low	Bad or inclimate weather can affect the team members trying to get to project meetings which will increase delays in the project	Plan ahead and look at the weekly forecast. If bad weather is coming up on a day that the team meets we should plan another day to get together

Summary

Total the number of observations. Summarize the observations, the associated risk levels, the recommendations, and any comments in a table format to facilitate the implementation of recommended controls during the risk mitigation process as summarized on the table above.

References

Accepting risk. (n.d.). Retrieved from https://www.investopedia.com/terms/a/accepting-risk.asp

itnow. (n.d.). *the importance of network monitoring*. Retrieved from itnow: https://itnow.net/the-importance-of-network-monitoring/

The importance of having firewall. (n.d.). Retrieved from https://www.geeksonsite.com/internet-security/the-importance-of-having-firewalls/