SUN TECHNOLOGIES

RISK ASSESSMENT REPORT

*11/18/2021*

*Version 1.1*

*Submitted by: Derick Ampadu*

Contents

[INTRODUCTION 3](#_gjdgxs)

[1.1 PURPOSE 3](#_30j0zll)

[1.2 SCOPE 3](#_1fob9te)

[1.3 Asset Identification 3](#_3znysh7)

[1.4 Threat Identification 3](#_2et92p0)

[1.5 Vulnerability Identification 3](#_tyjcwt)

[1.6 Risk Analysis](#_3dy6vkm) 4

[RECOMMENDATIONS 5](#_4d34og8)

[2.1 Corrective Actions Recommended 5](#_2s8eyo1)

[2.2 Estimated Timetable for Fixes 5](#_17dp8vu)

[2.3 Estimated Residual Risk 5](#_3rdcrjn)

[2.4 Future Recommendations 5](#_26in1rg)

[6](#_35nkun2)

# 

# **INTRODUCTION**

## ***1.1 PURPOSE***

The document provides Sun Technologies with an explanation of assets, threats and vulnerabilities to systems, data and networks. In addition, this document outlines recommendations for remediation to lower risks for Sun Technologies.

## ***1.2 SCOPE***

This risk assessment applies to the systems, data and networks of Sun Technologies.

## ***1.3 Asset Identification***

Sun Technologies assets consist of:

|  |  |  |
| --- | --- | --- |
| **Type**  **(System, Data, Network)** | **Description** | **Value**  **Cv (High, Medium, Low)** |
| Application (Widgets) | In-house developed specialty widgets | High |
| Databases | Microsoft SQL server. Used for storing of research data of company product, customer orders and customer information | High |
| Network equipment | Routers, firewall, switches, servers, monitors, cables, phones, wireless access points, printers etc. | Medium |
| Protocols | FTP used for file transmission/sharing. SSL used for transmission between client web browser and web server | Medium |
| Operating System | Microsoft Windows and Linux OS | Low |
| Server Room | Houses servers that hold critical company information, network equipment, cables, tools, spare utilities. | Medium |
| System Administrator | Individual responsible for managing network and systems as well as all IT requests. | Low |
| Office building | Physical location of the company which houses employees, computer equipment, paper documents, all point-of-sale items. | low |

## ***1.4 Threat Identification***

Sun Technologies threats consist of:

1. Malware – Malicious software such as spyware, ransomware, viruses and worms. These are normally activated when a user clicks on a malicious link or an attachment (UND, 2021)

* Encrypt access to network / system (ransomware)
* Activate malicious code without anyone knowing
* Install harmful software which causes damage in the short or long term

1. Inside threat – Disgruntled employee taking aim at the organization (TESU, 2018, mod. 6)

* Browsing of customer information
* Stealing from company
* Causing distraction to company network
* Injecting malicious code or viruses
* Data compromise
* Unauthorized access

1. Hackers – More specifically black hat hacker. These are individuals who use hacking techniques to breach systems to steal data, damage systems, or commit other cybercrimes such as using it for terrorist acts (Easttom, 2016)

* Unauthorized access
* Use of social engineering
* Spoofing
* System intrusion
* Data compromise
* Stealing of intellectual property
* Causing destruction to the network
* Causing Denial of Service attacks (DoS)

1. Environment – Environmental factors could also be a threat to the company in the event of natural disasters

* Hurricanes which could bring about flooding
* Fire damage
* Winter storm which sometimes brings down powerlines

## ***1.5 Vulnerability Identification***

Sun Technologies vulnerabilities consist of:

|  |  |
| --- | --- |
| Vulnerability | Description |
| Windows host is affected by multiple vulnerabilities on port 445 | Remote code execution vulnerability exists in Microsoft office due to improper validation of user supplied input before loading dynamic link library.  An attacker can use social engineering to get an employee to open a file where a well-crafted code could run and give access to the attacker. Windows remote host is missing security update KB4022715, multiple security bypass vulnerabilities exist with this. This is considered a critical finding |
| Anti-virus application not working properly. | McAfee VirusScan, an anti-virus application is installed on the remote host but isn’t working properly. This is considered a critical finding |
| Oracle database is affected by multiple vulnerabilities | Oracle Database Server is missing the July 2017 Critical Patch Update and therefore affected by multiple vulnerabilities. This is considered a high finding |
| The remote Windows host has a browser plugin installed that is affected by a type confusion vulnerability. | The remote Windows host is missing security update KB4049179. It is, therefore, affected by an unspecified type confusion flaw that is caused by input not being properly validated. This is considered a high finding |
| SSL certificated for server cannot be trusted. | The server's X.509 certificate cannot be trusted. This situation can occur in different ways, in which the chain of trust can be broken. This is considered a medium finding. |
| DNS server connection to internet | The company’s DNS is directly connected to the outside web with no protection. |
| No DMZ in network | There’s no presence of a demilitarized zone in the network configurations, this is a security concern. |
| Multiple databases and processes sharing one server | A database for orders and customer payment information is housed on a shared server, which also runs the Intranet |
| One system administrator | There’s only one system administrator with no backup or immediate replacement |
| No internal firewall | With the DNS server connected directly to the outside web, it will be easy for an attacker to gain access to the internal network since there’s no internal firewall to block malicious attackers. |
| Power outages | Normally caused by winter storms, hurricanes or flooding which brings down lines |

## ***1.6 Risk Analysis***

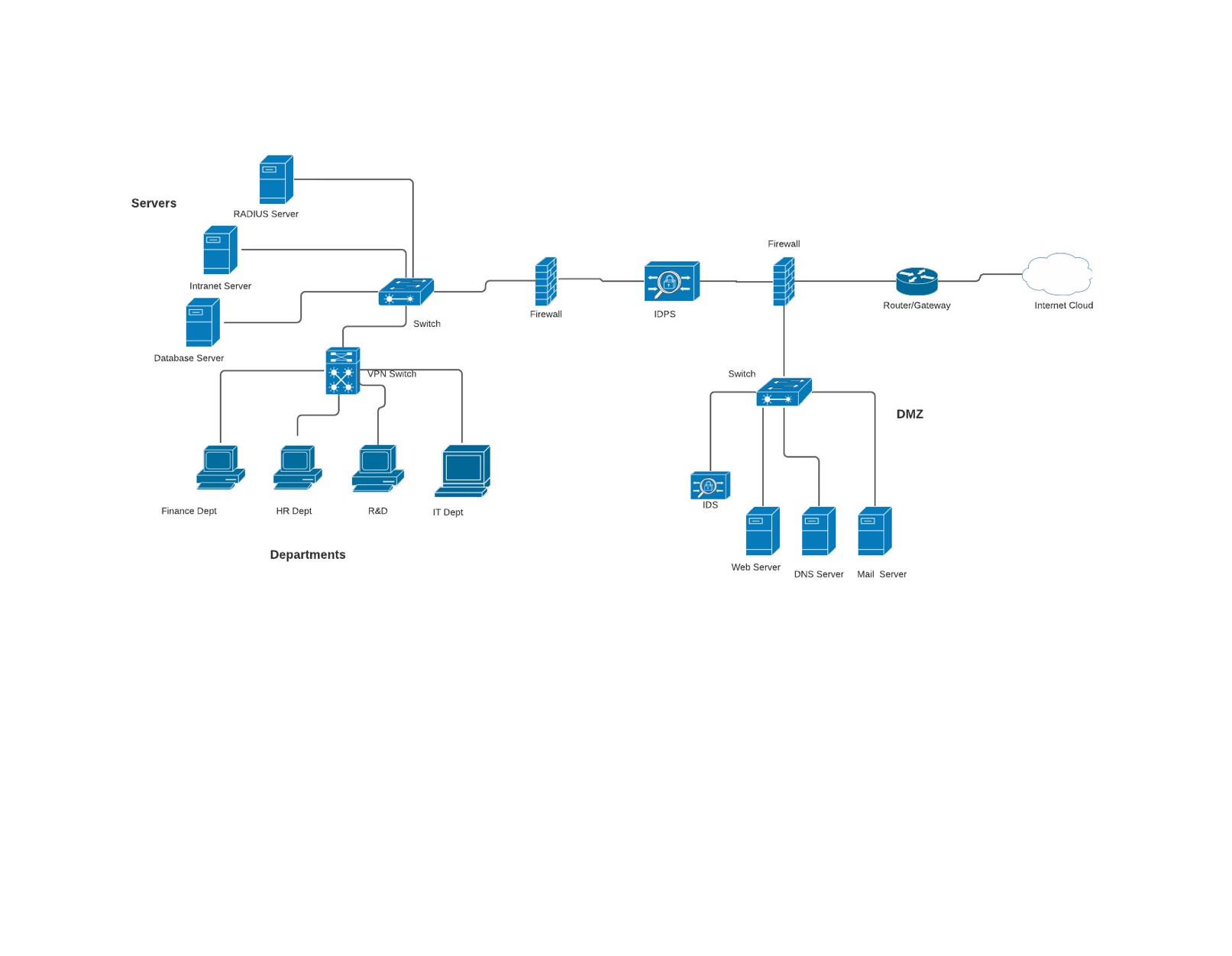
Sun Technologies risks consist of:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Risk Name** | **Risk Description** | **Mitigations Already in Place** | **Potential Mitigations to Implement** | **Risk Level**  **(high, med, low)** |
| DNS poisoning | Hacker manipulating known vulnerabilities with the domain name system (DNS) | None | Place DNS server in a DMZ behind a firewall and not directly connected to the web | High |
| No disaster recovery plan | Disaster recovery plan (DRP) are needed in case of an event or incident | Weekly backups | Develop and test a disaster recovery plan | Medium |
| Windows remote host can be exploited | Attackers can gain access through a vulnerable remote host | None | Apply security update KB4022719 or KB4022722. | High |
| CIA triad compromise | Data could be accessed by unauthorized employees. Confidentiality could be broken and integrity of the data could be lost. | Authentication | Place customer Personally Identifiable Information as well as customer orders on different server from the shared intranet server | High |
| Login compromise | Employees allowed to work from home could have their logins compromised if working from a public space | Passwords | Provide a secure VPN tunnel for employees to connect to company resources, employees should use strong password as a safety precaution, provide a RADIUS server for authentication whenever an employee tries to login. Also use multi-factor authentication | Medium |
| System admin could become complacent | Company employs only one system admin. He/she could become complacent, overworked or could have too much power and cause harm | None | Hire another network/system admin to help relieve work burden as well as job rotations | Low |
| Virus Infecting system/network | Malware including viruses, spyware, ransomware would be able to infect system causing financial loss to the company | McAfee Antivirus | Implement patch management and apply security updates on time, utilize good antivirus to prevent system from virus infection. | High |

Overall, the company has a high-risk level which makes it very susceptible to outside attacks from hackers, malwares and insider threats. The DNS server which is placed outside of the network, makes it easy for attackers to bypass the firewall to the internal services. The network has no defense-in-depth strategy in place to help mitigate attacks, also, the system administrator is not keeping up with updates and patches according to results from the scan which makes it easy for viruses to get through the network.

# **RECOMMENDATIONS**

## ***2.1 Corrective Actions Recommended***



Above is the new redesigned network diagram for Sun Technologies. This new diagram is a revamp of the old network diagram, with new added features which will improve the overall security posture of the company. A defense-in-depth approach used, which should help improve the company’s overall network to prevent unwanted traffic and deter other forms of threats. The recommendations are as follows:

* Two firewalls are recommended. The first being a perimeter firewall which a secured boundary providing the main defense between the private network and the internet. This will be the first line of defense for the company’s network should any unwanted traffic or potentially dangerous code tries to penetrate. The second firewall also known as the internal firewall, is security solution designed to protect a network from attacks that have already breached the perimeter firewall. The internal firewall is more hardened, highly restrictive and more advanced than the perimeter firewall in order to intelligently detect malicious activities (VMWare, 2021).
* Next recommendation would be having a Demilitarized Zone (DMZ). DMZ or demilitarized zone, is a physical or logical subnet that separates a local area network (LAN) from other untrusted networks, usually the public internet (Lutkevich, 2021). DMZ networks are areas where services which are provided to users on the public internet are place, this is why we placed our Web server and DNS server there. Servers and resources in the DMZ are accessible from the internet, but the rest of the internal network is protected. So, in this case DMZ acts as an additional layer of security for our LAN. This would be a safe zone where customers can access the company’s website to place their orders, check statuses and interrupt with tech support if needed without having access to the company’s internal resources. Also, employees will be able to reach the mail server in the DMZ at all times, and in the event where an employee is connected to a malicious Wi-Fi, whereby they login to check their mail, the internal network of the company will be protected from any malicious activities from getting in.
* Another security device in the DMZ is the IDS also known as Intrusion Detection System. The job of the IDS is to monitor suspicious activities and log it. In some cases, it notifies the administrator if it’s configured to do so. If an attacker is able to breach our outer firewall, and ends up in our DMZ, the IDS should be able to pick up the activities, log it and send a notification to our terminal computer in the IT department.
* An IDPS (Intrusion Detection and Prevention System) is a hybrid device which serves as an intrusion detection and intrusion prevention system at the same time. IPS just like the IDS is a security device which inspects all inbound and outbound port activities on a machine/firewall/system and looks for patterns that might indicate an attempted break-in (Easttom, 2016). The IPS takes this a little further, it’s able to detect and shut down malicious communications. For this reason, the IDPS which can both detect and shut down malicious communications is placed in-between the firewalls, to prevent any malicious traffic before it reaches the inner firewall.
* A big security concern that was found during the network upgrade was, Sun Technologies housed customer orders and payments information on a shared, which also runs the intranet. In the event where an attacker is able to compromise the network, it will be easy to steal customer information which normally includes; names, addresses and credit card information as well as employee information since they are all stored on the same server. Loss of customer information could trigger a multitude of law suits and this will be detrimental to the company. Another concern would be, employees who work in other departments and are not authorized to see customer information will all have access since the information is on the shared server. This goes against CIA triad (confidentiality, integrity and availability). These three principles are a model to guide policies for information security. The confidentiality part relates to ensuring that data is not accessed by individuals who are not authorized to see the data (TESU, 2018, mod. 2). Strategies such as least privilege should be implemented. With least privilege, a level of access is given to an individual to complete his/her duties and no more (TESU, 2018, mod. 2). Also, two recommended servers have been created in the above diagram, one would serve solely as a database server which will house customer orders and customer payment information and the other server houses the intranet.
* Sun Technologies currently employs one system administrator who maintains the network. This could be a security concern in many ways. This one employee could be an inside threat to the company if he/she decides to go rogue if they felt the company has treated them unfairly in one way or another. Customer data could be stolen; systems could be destroyed and most importantly this individual can be stealing company resources. In the above suggested network, an IT department is added and it’s being recommended to the company to hire another system/network administrator to share the duties with the one employee. This could benefit the company in so many ways, some of the benefits include; SoD (segregation of duties) and job rotation. SoD ensures that one individual does not have all the power for a certain task, an example would be if one person initiates a workorder for a part, a second individual can approve it when SoD is put in place (TESU, 2018, mod. 2). Also, Job rotation would ensure that one person will not maintain in the same position for a long time where they may get too comfortable which could bring about complacency in certain situations (TESU, 2018, mod. 2). Another benefit would be, the company will have enough IT staff to help run the network and system and also be able to help resolve customer and employee issues in a timely manner.

## ***2.2 Estimated Timetable for Fixes***

Currently, there are patches available for the vulnerabilities found in the vulnerability scan which was performed. These patches should be implemented as soon as possible for the critical and high vulnerabilities. For medium and low vulnerabilities, it should be fixed with the next 30 days from the time of report. prevent any major incident from happening.

## ***2.3 Estimated Residual Risk***

With the risk factors laid out in this report and corrective actions recommended, it should be noted that the company will still be susceptible to residual risk. Residual risk is the risk that remains in place after security measures and controls have been put in place (Whistic, 2019). After all vulnerabilities noted have been addressed, it is estimated that employee errors pose as residual risk to the company. If employees are not properly trained on security measures and the implications their errors (such as using public Wi-Fi to log into company system, clicking on unknown attachments etc.) may have on the company, then the company will be at a disadvantage in ensuring a secured network.

## ***2.4 Future Recommendations***

These are a few future recommendations which should be implemented by the company to help improve the company’s overall security posture;

1. Implement a Disaster Recovery Plan with strong consideration for a hot or warm site to help the company recover faster if an incident is to happen.
2. Implement a patch management system whereby all software patches are checked and done when they become available to avoid viruses.
3. Perform vulnerability scans quarterly, document findings and act on findings to prevent any serious events from happening
4. Perform risk assessments annually and document process
5. Hire another system admin to help with workload
6. Provide security training for employees with yearly refreshers to keep them up to date on security trends and information that could help prevent phishing attacks or viruses.

# **REFERENCES**

UND. (2021). *7 types of cybersecurity threats*. Retrieved from

https://onlinedegrees.und.edu/blog/types-of-cyber-security-threats/

Easttom, C (2016). *Computer Security Fundamentals (3rd ed.).*Pearson Education, Inc.

VMWare, Inc. (2021). *Internal Firewall.* <https://www.vmware.com/topics/glossary/content/internal-firewall>

VMWare, Inc. (2021). *Perimeter Firewall.* <https://www.vmware.com/topics/glossary/content/perimeter-firewall>

Lutkevich, B. (2021, July). *DMZ in Networking*. <https://searchsecurity.techtarget.com/definition/DMZ>

TESU [Course Resources]. (2018, April). *Introduction to Cybersecurity*. Retrieved from <https://docs.google.com/document/d/1i1m5UxvGLAFM0ePi6OH2q1vwwyUbzn-tQGLNmiK_Vgw/edit>

Whistic. (2019, January). *Residual Risk: What Constitutes an Acceptable Level of Risk?* https://blog.whistic.com/residual-risk-what-constitutes-an-acceptable-level-of-risk-5cea7144f08d