Application of computer, network and information security techniques

Jessica Fealy

# Abstract

This report will discuss the impacts and ways to mitigate against attacks to a computers information, network and data systems. A method on how to create a plan to implement new security protocols will also be explained. Topics such as malware, SQL injections, static and dynamic packet filtering, encryption, and securing different server roles will be discussed and explained throughout this report.

Table of Contents

[Abstract 0](file:///C:\Users\Vnvjvjvh\Documents\University\2.%20Year%201\Information%20and%20security\Alex\Assignment%201%20-%20Report\18024092.docx#_Toc29504101)

[Introduction 2](#_Toc29504102)

[Computer Security 2](#_Toc29504103)

[Main vulnerabilities, threats, and attacks to system security in the organisation 2](#_Toc29504104)

[Suggest some techniques that the company’s in-house developers could employ to make software more secure. 3](#_Toc29504105)

[Network Security 3](#_Toc29504106)

[Network infrastructure server roles that need to be secured in a typical SME network 3](#_Toc29504107)

[Packet filtering firewalls 4](#_Toc29504108)

[Physical protects to ensure the physical security and availability of a server 5](#_Toc29504109)

[Information Security 5](#_Toc29504110)

[Principles of data encryption and provide examples of how this can be implemented 5](#_Toc29504111)

[Strategy for implementing information security in the organisation 6](#_Toc29504112)

[Bibliography 8](#_Toc29504113)

[Computer Security References 8](#_Toc29504114)

[Network Security References 8](#_Toc29504115)

[Information Security References 9](#_Toc29504116)

# Introduction

Throughout this report we shall be discussing the ways in which an organisation computer system may be attacked and who are the most likely actors, and the best way to mitigate against attacks and how to mitigate against various actors. Additionally, discussions will occur based on the best server security practices with both software and hardware protective strategies in which an organisation can employ. Finally, we shall be talking about how an organisation can best protect their data against unauthorised breaches and devising a plan an organisation can implement to construct a security system strategy that best matches their needs.

# Computer Security



## Main vulnerabilities, threats, and attacks to system security in the organisation

A computer system inherently has multiple vulnerabilities that leave the systems are risk, these vulnerabilities are categorised in hardware vulnerabilities and software vulnerabilities (WhatIs.com, 2015).

Hardware vulnerabilities are exploits in a computer that allows a malicious actor to access systems through a remote connection or a physical connection. An example of a hardware exploit is having older storage drives which lack a self-encryption process, without such feature a malicious actor with physical access to an organisations computer systems do not require any special equipment to access the drives data, they only need to remove the storage drives from computers / serves to have unrestricted access to an organisations data (Lindros, 2016).

A software vulnerability can be defined as such “A software vulnerability is a glitch, flaw, or weakness present in the software or in an OS” (Mohanty, 2018). Input validation error occurs when a program fails to validation an input from the user, this can be as simple as not checking for the correct data type being entered that causes a system crash, to a more malicious attack called a SQL (**Structure Query Language**) injection. An SQL injection works by code being entered into a text box which an unsecured program would allow to run. This code entered can copy databases with all personal data or an organisation complete database (Mohanty, 2018),

There are ever-increasing threats that an organisation must defend against. One of the most common threats that an organisation would face is computer malware. Malware is a broad computer term which covers many different types of programs, although all these programs can be defined as such “designed to infiltrate and damage computers without the users’ consent” (Bullguard.com, n.d.). An example of malware is ransomware, there has been a recent surge in popularity of this type of attack. Ransomware operates on the principle of covertly gaining access to a computer system, like any other malware this can happen through compromised email file or web files. Once ransomware has gained access to a computer, the program will begin encrypting all the data and making the computer unfunctional until the organisation pays a fee (commonly in a cryptocurrency) to have their data decrypted (GeeksforGeeks, n.d.).

While malware is the most common type of threats that an organisation will face, they are not the only type. Vulnerabilities can occur with out of data software, most commonly these security flaws are discovered in a prompt manner and a security patch is released to fix such a flaw. The burden lays upon the system admin of an organisation to ensure these patches are installed to ensure there are no backdoors in the company’s computer systems. An out of date program can allows malicious actors to gain access / infiltrate an organisations system (Ciunci, 2016).

An attack to an organisation has the goals to gain unauthorised access, or to cause interruption / damage to the organisations ability to operate. Attacks on an organisation could crash their servers. This is done by preforming a DDoS (**Distrusted Denial of Service**) attack, this attack targets a specific server or a cluster of servers by using a botnet (a botnet is a large group compromised computers) to interrupt and overwhelm servers prevent normal traffic to reach their destination. Such attacks can prevent the organisation from preform business online until the attack is over (Cloudflare, n.d.).

Other attacks can come from the organisation’s own employees. An insider malicious actor is the most common attacker that can impact a business. Upset employees, or bitter ex-employees with privileges to the organisation systems can cause serious damage. An insider actor is likely to have privileges to key or sensitive areas unrestricted, with such access they can install malware onto the computer systems or download sensitive materials such as customer personal information.

An organisations key concern when implementing a new computer security procedure is the impact on the balance of accessibility and the overall security. A general rule is that with increased security the systems will become less accessible to the users. For example, a computer system that is disconnected from the internet completely negates the risk from internet-based attacks, yet this prevents the employee to use the computer systems in a real-world situation. However, a policy that enforces all employees use a secure long password, this leaves the computer systems more secure than a shorter password while having a minimal impact on the availability to the systems.

## Suggest some techniques that the company’s in-house developers could employ to make software more secure.

An organisation can employ a multitude of methods to ensure software is secure. An organisation can simply design test conditions that would cause an insecure program to become compromised, testing a software’s input validation will ensure that basic attacks have no effect.

Additional ways in which an in-house development team can secure their software is by implementation strict privileges, this is preventing anyone without the need of access a certain system from accessing that system. Doing so limits the damage that a disgruntled employee can have when attacking the systems.

A final keyway in which an organisation can ensure their software is secure is by constantly doing bug fixes and patches. It is inevitable that a software will develop a bug, or a bug is found long into the software’s use. Whenever these are found it is paramount that an organisation fixes these to prevent a security flaw which a malicious actor can abuse.

# Network Security

## Network infrastructure server roles that need to be secured in a typical SME network

There are several types of servers in which an organisation can employ to do a various of tasks, these include a website server, an email server, and database servers (Webopedia, 2011). These are just three examples of servers that a user can use, but these three are the most universal servers for any organisation.

Each server is an area of vulnerability for an organisation thus it is vital they ensure the security of each server. A mail server faces the vulnerabilities of mail deliverable malware and spam (Apriorit, 2019) , way to mitigate against these threats is by having the mail server scan all incoming and outgoing transmissions for potential malware and warning the recipient to not open the file, or block the transmission; the server can also scan for any bulk emails being received and block these.

A date server is usually an organisation most expensive assets thus needs to be heavily secured. There are a few ways an organisation can go about securing this; however, the most common way is to encrypt all the data stored on the server. This means even in the event of a breach no important data can be stolen.

A web server is the where the organisation hosts their online presence, this server will have to front the most of attempted breaches. An organisation should use protocol such as HTTPS (**Hypertext Transfer Protocol Secure**), this encrypts all transmissions between the sever and the end user.

An organisation with a higher expendable security budget may wish to invest in security server infrastructure. Using this an organisation can have any camera footage streamed and saved to these servers and using the server can remotely access camera feeds. As security servers are the backbone to physical servers it is imperative that these are very well protected both physically and digitally.

While each server has their own specialised security method, all servers can also be secured with common methods. A popular security method is by using a VPN (**Virtual Private Network**). A VPN is used to encrypt all data being transmitted and hides the end route from an ISP (**Internet Service Provider**)and any malicious actors trying to monitor a company’s network transmissions. Using a VPN all these actors will see is the VPN server destination and the size of data transmission, they are unable to see what the content of the transmissions. Additionally, keeping offsite back up servers is advisable in the event the primary servers are damaged or corruption of data.

## Packet filtering firewalls

Packet-filtering a type of firewall that monitors incoming and outgoing transmissions of packets depending on a rule set which operates on the third levels of the OSI model. This firewall will analyse the packets incoming source internet protocol (**IP**) address (source address) and the outgoing packets IP address (destination address), depending on the ruleset set for the firewall there will be a decisions whether or not the source or destination address is considered trusted / secure. Additionally, with analyzing the source and destination address the firewall will also consider the protocol being used to transmit the packets (e.g. TCP/IP), and the ports in which the packets are being sent thought / sent to (Techopedia, n.d.).

One method of packet-filtering is called static filtering. This form of firewall offers an efficient and fast firewall, however the speed that this firewall offers comes with a payoff to the security (Sciencedirect.com, n.d.). Due to the fact a static filtering method is a simply a Boolean choice, there is no consideration for the contents of the packets. This means while the destination, ports and protocols could be considered trusted and secure the content are insecure or compromised. Another form of packet filtering is called stateful or dynamic packet filtering, this method differs to static due dynamic using context and taking the entire transmission into account rather than just the individual packet and detecting unusual traffic behavior.

The primary advantages to static packet filtering is the efficiency and speed in which the firewall can determine whether to allow packets to pass through the firewall while still maintaining reasonable security. This is due to the firewalls Boolean process with only allow or disallow depending on the ruleset. Another advantage is the ease that a packet firewall can be implemented on servers, this is due to many routers and servers supporting this form of firewall (Etutorials.org, n.d). Whereas, the advantages for dynamic packet filtering is the increased security benefit from being able to investigate the complete transmission, doing this is resource intensive activity, this is primarily why organisations choose static over dynamic.

The primary disadvantages to static packet filtering is the complex process of creating and maintaining the firewalls ruleset. The user must have a complete understanding of TCP/IP protocols and all their headers. Incorrectly initialing the ruleset can either prevent traffic which you intended to allow or allow traffic in which you intended to prevent. Another disadvantage is that packet filtering has limited abilities to create logs of incoming and outgoing transmissions in level 3 and 4 of the OSI model, this mean while a network admin would be able to see an attempted attack which was denied, the would be able to determine what the attack was intended to do (Etutorials.org, n.d).

## Physical protects to ensure the physical security and availability of a server

Physically protecting a server is just as important as virtually protecting a server. If unauthorised personnel have unrestricted access to an organisation’s computer, they can cause mass amount of damage. Thus, organisations must divert efforts and funds to protect these servers. An organisation can implement minor physical security such as a key locked room or key locked cage, to more secure and complicated methods such as biometrically locked rooms in highly secured and guarded locations (HPE, 2018).

Servers are not designed to have their power interrupted; such interruptions can cause corruption of data. A tool called an uninterruptible power supply (**UPS**) is essentially a larger battery, this tool gives a server a limited supply of electricity which is enough for the sever to preform a safe shut down. Servers should be in a well-ventilated room, due to server rooms usually be host to more than one server, with all of them being functional 24/7 heat become a major factor, ensuring adequate ventilation and cooling are a must to ensure the longevity of hardware. Finally, server rooms must be installed with fire suppressant systems, in the event of a fire hard disk drives (**HDDs**) are likely to be damaged with potential data lose, fire suppressant will mitigate this potential risk.

An additional way to protect an organisations server is disable or block any data ports on the server accessible from this front. This means that accidentally plugging a potentially dangerous drive or being able to copy data physically will be difficult. Leaving any data connection on the rear of the servers will mean that only server technicians who are aware of these ports’ functionality are able to use them for server maintenance.

An organisation should subscribe to other common security measures, these include installing and maintaining camera in the server room and in the surrounding areas, keeping logs of all personnel who enter the server room, and by training staff both on common attacks to be vigilant about and training them to report any suspicious persons or activity around the server rooms.

Finally, for a company to ensure the availability of the servers and their connections to the outside internet, it is advisable for them to have multiple data connections to their ISP which take separate physical routes. This is because if construction works or other activity outside the organisations controls disrupts one data connection, there are back up connections which allow internet access. This same idea can be applied for connecting to the remote back up servers.

# Information Security

## Principles of data encryption and provide examples of how this can be implemented

Data encryption is the act of converting plain text to cipher text. This cipher text is unreadable without knowing the method of encryption used and the key used. Data encryption is a preventive measure to protect data when in non-authorised procession, this is to protect the privacy and confidentially of the data. For encryption to be beneficial both sender and recipient must be easily able to decipher the ciphertext, while also being near impossible for anyone else to decrypt.

Two primary data encryption methodologies exist, these are symmetrical and asymmetrical. Where these two methodologies diverge is in their manner of handling keys. With symmetrical encryption is the older methodology and boasts more efficient and quicker encryptions which is beneficial to a computer system by decreasing CPU usage. For symmetrical encryption to work both parties use the same secret key to decrypt the data, while setting a symmetrical encryption up is relativity easy if the secret key is stolen then all the data can no longer be considered secure as anyone could decrypt the data (Cryptomathic, 2019). While asymmetrical encryption is more resource intensive than symmetrical but this increased demand in resources all allows for an increased level of protection. This method of encryption uses 2 keys, one private and one public. The public key is used to encrypt the data, with the private key being used to decrypt the data (SSL Certificates, n.d.).

Each asymmetric and symmetric encryption have their more popular encryption algorithm. For asymmetric this is RSA (**Rivest-Shamir-Adelman** these are the 3 creators of the algorithm). RSA has become the industry standard for encrypting data when transmitting over the internet (Webopedia, n.d.). The advantages of RSA are the very secure nature of the algorithm, this is due to complex maths being preformed to create the encryption keys and cipher text, doing this ensures the encryption is very difficult to decrypt (Rouse, n.d.). While with this high level of security comes a downfall regarding the resources required to do the mathematic functions effectively. Regarding symmetric the industry standard encryption is AES (**Advanced Encryption Standard**), this is used by governments to encrypt their data. AES is regarded to be highly secure and reliable. However, with AES key leakage can occur, this is where is the private key is stolen meaning all data using this key can be decrypted by unauthorised users (Cryptomathic, 2019).

## Strategy for implementing information security in the organisation

For an organisation to correctly implement a fully developed and suited strategy there are 6 vital steps they must fulfil, this is called the SDLC (**System Development Life Cycle**) waterfall methodology. These steps are investigation, analysis, design, implementation, testing, and maintenance.

Investigation - For an organisation to determine if their security is acceptable with a feasibility analysis to determine whether an updated security plan is required. They then must investigate every aspect of their organisation. They question what their current threats are and who those threat actors may be. They must determine if their current data controller is of a suitable position in the organisation, when they last trained their staff on security practices, also investigating the current privilege levels will need to be determined. During this phase the organisation must all determine what their available budget is, for a SME it is assumed that their available security budget low.

Analysis – After an organisation have completed their investigation determine how to prioritise their security requirements, due to budgetary constants a SME will need to fix the biggest security flaws first, and if their budget is allowing focus on the small flaws, also determining if the current data controller and if the current privileges are up to their security requirement are vital. For example, a SME may decide to train staff in secure practices before improving their potentially already adequate physical server protections.

Design – Once an analysis has been sorted, the organisation can begin to plan exactly what requirements the software, hardware and staff training need to be. Software improvement (as spoken in this report) can be improving anti-virus, VPNs, planning on what personnel will have privilege promotions and what personnel need a demotion, and what encryption protocols they want to use. For hardware requirement the organisation will need to decide where they want to prioritise their budget. For a lower budget SME hardware improvement such as locked server rooms will improve security, but for SME for a more dedicated security budget they can invest in camera and biometric locks. Staff training is key in protecting an organisations security, staff training around being safe online and common malware attacks can greatly decrease breaches. Other training around common social engineering tactics can help to prevent stolen passwords or company information. Additionally, in this stage the organisation must choose who will become the data controller, it is advisable for this to be the CTO or CEO.

Implementation – After the organisation has completed a design and requirement of what they want to add and improve to their security they will begin to implement. They will need to send staff off from training, while this is happening it is advised that the organisation also implement the new software and hardware changes, this will decrease the impact on the employee’s ability to work.

Testing – Now that all the improvement has been made the organisation must test to determine if the changing have made improvement to their security. An organisation can either preform these tests internally or externally. With internal testing the system admin will try breach the computer as if they were malicious actors, while this is low cost it can be ineffective as the system admins may avoid security flaws. External testing removes the bias nature of internal, with the draw back of being expensive.

Maintenance – This stage is about ensuring that the organisations security procedures are still effective long term, ensuring that employees keep having their training refreshed with any vulnerabilities the organisation may encounter, to keep all software patched / updated such as the operating system, and to ensure that malware security definitions are updated regularly. If it is determined that the security producers are no longer effective, then the organisation can repeat the previous steps to improve their security.

# Bibliography

## Computer Security References

WhatIs.com. (2015). *What is hardware vulnerability? - Definition from WhatIs.com*. [online] Available at: https://whatis.techtarget.com/definition/hardware-vulnerability [Accessed 8 Dec. 2019].

Lindros, K. (2016). *12 hardware and software vulnerabilities you should address now*. [online] Computerworld. Available at: https://www.computerworld.com/article/3130119/12-hardware-and-software-vulnerabilities-you-should-address-now.html [Accessed 8 Dec. 2019].

Mohanty, S. (2018). *5 Important Software Vulnerabilities - DZone Security*. [online] dzone.com. Available at: https://dzone.com/articles/5-important-software-vulnerability-and-attacks-tha [Accessed 8 Dec. 2019].

Bullguard.com. (n.d.). *A definition of malware*. [online] Available at: https://www.bullguard.com/bullguard-security-center/pc-security/computer-threats/malware-definition,-history-and-classification.aspx [Accessed 8 Dec. 2019].

Ciunci, M. (2016). *Top 5 Vulnerabilities in Your Organization's Computing System*. [online] I.S. Partners. Available at: https://www.ispartnersllc.com/blog/5-common-vulnerabilities-organizations-computing-system/ [Accessed 5 Nov. 2019].

GeeksforGeeks. (n.d.). *What is WannaCry? How does WannaCry ransomware work? - GeeksforGeeks*. [online] Available at: https://www.geeksforgeeks.org/what-is-wannacry-how-does-wannacry-ransomware-work/ [Accessed 8 Dec. 2019].

Schick, S. (2017). *Insider Threats Account for Nearly 75 Percent of Security Breach Incidents*. [online] Security Intelligence. Available at: https://securityintelligence.com/news/insider-threats-account-for-nearly-75-percent-of-security-breach-incidents/ [Accessed 5 Nov. 2019].

Cpni.gov.uk. (n.d.). *Insider risk | Public Website*. [online] Available at: https://www.cpni.gov.uk/insider-threat [Accessed 5 Nov. 2019].

Cloudflare. (n.d.). *DDoS Learning Objectives*. [online] Available at: https://www.cloudflare.com/en-gb/learning/ddos/what-is-a-ddos-attack/ [Accessed 8 Dec. 2019].

## Network Security References

Sciencedirect.com. (n.d.). *Packet Filtering Firewall - an overview | ScienceDirect Topics*. [online] Available at: https://www.sciencedirect.com/topics/computer-science/packet-filtering-firewall [Accessed 22 Dec. 2019].

Techopedia.com. (n.d.). *What is Packet Filtering? - Definition from Techopedia*. [online] Available at: https://www.techopedia.com/definition/4038/packet-filtering [Accessed 22 Dec. 2019].

Rouse, M. (2009). *What is stateful inspection? - Definition from WhatIs.com*. [online] SearchNetworking. Available at: https://searchnetworking.techtarget.com/definition/stateful-inspection [Accessed 22 Dec. 2019].

Etutorials.org. (2020). *Firewall Categories :: Chapter 2. Introduction to Firewalls :: Part I: Security Overview and Firewalls :: Router firewall security :: Networking :: eTutorials.org*. [online] Available at: http://etutorials.org/Networking/Router+firewall+security/Part+I+Security+Overview+and+Firewalls/Chapter+2.+Introduction+to+Firewalls/Firewall+Categories/ [Accessed 5 Jan. 2020].

Webopedia. (2011). *Server Types*. [online] Available at: https://www.webopedia.com/quick\_ref/servers.asp [Accessed 7 Jan. 2020].

Apriorit. (2019). *Mail Server Security: Potential Vulnerabilities and Protection Methods*. [online] Available at: https://www.apriorit.com/qa-blog/428-mail-server-security-testing [Accessed 7 Jan. 2020].

HPE. (2018). *Secure your server room*. [online] Available at: https://www.hpe.com/us/en/insights/articles/how-to-secure-your-server-room-1809.html [Accessed 7 Jan. 2020].

## Information Security References

Cryptomathic, P. (2019). *Symmetric Key Encryption - why, where and how it’s used in banking*. [online] Cryptomathic.com. Available at: https://www.cryptomathic.com/news-events/blog/symmetric-key-encryption-why-where-and-how-its-used-in-banking [Accessed 5 Jan. 2020].

SSL Certificates. (n.d.). *What is Asymmetric Encryption? Read Symmetric vs. Asymmetric Encryption Diversity*. [online] Available at: https://cheapsslsecurity.com/blog/what-is-asymmetric-encryption-understand-with-simple-examples/ [Accessed 5 Jan. 2020].

Webopedia. (n.d.). *What is RSA? Webopedia Definition*. [online] Available at: https://www.webopedia.com/TERM/R/RSA.html [Accessed 7 Jan. 2020].

Rouse, M. (n.d.). *What is RSA algorithm (Rivest-Shamir-Adleman)? - Definition from WhatIs.com*. [online] SearchSecurity. Available at: https://searchsecurity.techtarget.com/definition/RSA [Accessed 7 Jan. 2020].

Cryptomathic. (2019). *Symmetric Cryptography and Key Management: Considerations on Key Exhaustion, Rotation and Security Models*. [online] Available at: https://www.cryptomathic.com/news-events/blog/symmetric-cryptography-and-key-management-considerations-on-key-exhaustion-rotation-and-security-models [Accessed 7 Jan. 2020].