UNIVERSITY of GREENWICH
Alliance with FPT Education

BTEC

Higher Nationals in Computing

UNIT 5

SECURITY

ASSIGNMENT

No.1

Learner's name: Trinh Thi Dieu Huyen

Assessor name: Dang Thai Doan

Class: GCS0801B.2

Learner's ID: GDD18606

Subject's ID: 1623

Assignment due: May 2020

Assignment submitted: May 2020

Assessment Brief

Qualification	**BTEC Level 5 HND Diploma in Computing**		
Unit number	Unit 5: Security		
Assignment title	Security Presentation and Guidebook		
Academic Year	2020		
Unit Tutor	Dang Thai Doan		
Issue date	May 2020	**Submission date**	May 2020
IV name and date	Dang Thai Doan		

Submission Format
The submission is in the form of two documents/files: 1. A ten-minute Microsoft® PowerPoint® style presentation to be presented to your colleagues. The presentation can include links to performance data with additional **speaker notes** and a **bibliography using the Harvard referencing system.** The presentation slides for the findings should be submitted with speaker notes as one copy. 2. A detailed report that provides more thorough, evaluated or critically reviewed technical information on all of the topics. You are required to make use of the font **Calibri, Font size 12, Line spacing 1.5, Headings, Paragraphs**, **Subsections and illustrations** as appropriate, and all work must be **supported with research and referenced** using the **Harvard referencing system.**

Unit Learning Outcomes
LO1 Assess risks to IT security. **LO2** Describe IT security solutions.
Assignment Brief and Guidance
You work as a trainee IT Security Specialist for a leading Security consultancy in Vietnam called FPT Information security FIS. FIS works with medium sized companies in Vietnam, advising and implementing technical solutions to potential IT security risks. Most customers have outsourced their security concerns due to lacking the technical expertise in house. As part of your role, your manager Jonson has asked you to create an engaging presentation to help train junior staff members on the tools and techniques associated with identifying and assessing IT security risks together with the organizational policies to protect business critical data and equipment. In addition to your presentation you should also provide a detailed report containing a technical review of the topics covered in the presentation. Your presentation should: 1. **Identify** the security threats FIS secure may face if they have a security breach. Give an example of a recently publicized security breach and discuss its consequences 2. **Describe** a variety of organizational procedures an organization can set up to reduce the effects to the business of a security breach. 3. **Propose** a method that FIS can use to prioritize the management of different types of risk 4. **Discuss** three benefits to FIS of implementing network monitoring system giving suitable reasons. 5. Investigate network security, **identifying** issues with firewalls and **IDS** incorrect configuration and **show** through examples how different techniques can be implemented to improve network security. 6. **Investigate** a 'trusted network' and through an analysis of positive and negative issues determine how it can be part of a security system used by FIS. Your detailed report should include a summary of your presentation as well as additional, evaluated or critically reviewed technical notes on all of the expected topics.

<table>
<tr><th colspan="3">Learning Outcomes and Assessment Criteria</th></tr>
<tr><th>Pass</th><th>Merit</th><th>Distinction</th></tr>
<tr><td colspan="2">LO1 Assess risks to IT security</td><td rowspan="5">LO1 & 2
D1 Investigate how a ‘trusted network’ may be part of an IT security solution.</td></tr>
<tr><td>P1 Identify types of security risks to organisations.
P2 Describe organisational security procedures.</td><td>M1 Propose a method to assess and treat IT security risks.</td></tr>
<tr><td colspan="2">LO2 Describe IT security solutions</td></tr>
<tr><td>P3 Identify the potential impact to IT security of incorrect configuration of firewall policies and third-party VPNs.
P4 Show, using an example for each, how implementing a DMZ, static IP and NAT in a network can improve Network Security.</td><td>M2 Discuss three benefits to implement network monitoring systems with supporting reasons.</td></tr>
</table>

Assignment Front Sheet

Qualification	**BTEC Level 5 HND Diploma in Computing**		
Unit number and title	**Unit 5: Security**		
Submission date	May 2020	**Date Received 1st submission**	May 2020
Re-submission Date		**Date Received 2nd submission**	
Student Name	Trinh Thi Dieu Huyen	**Student ID**	GDD18606
Class	1623 GCS0801B.2	**Assessor name**	Dang Thai Doan
Student declaration I certify that the assignment submission is entirely my own work and I fully understand the consequences of plagiarism. I understand that making a false declaration is a form of malpractice.			
		Student's signature	Dang Thai Doan

Grading grid

P1	P2	P3	P4	M1	M2	D1

❒ **Summative Feedback:**		❒ **Resubmission Feedback:**
Signature & Date:		

Table of Contents

Table of figure

Introduction.

- ✓ Identify, introduction and assess IT security risks. Give examples and expand.
- ✓ Provide some information on the impact of those risks and the best / most practical solutions to solve the problem.
- ✓ Research the benefits of security tools.

LO1 Assess risks to IT security.

Risk can be simply understood as something or someone capable of posing danger, difficulty or threat to the problem. Specifically, there are risks such as data in computers, stolen servers, etc.., during your use of that data.

P1 Identify types of security risks to organizations.

In computer security, a threat is a danger that can exploit vulnerabilities to breach security. Today, security-related issues are extremely urgent and important. New threats appear almost daily. If we can monitor and prepare "how to deal" with these threats, we can prevent, improve resilience or support our goals.

1. Naturally occurring risks

Is caused by nature causing you to lose Important data. This is a threat to your data because you don't know when your data was lost because it was naturally hard to predict.

Figure 1: Naturally occurring risks

Example: Suppose you are working at the company and important data exists only on that computer. Suddenly a fire occurs, the fire alarm system will operate and water will appear. If you can carry your computer with you run away, your computer will be damaged by water, but you can recover a little data. If you cannot bring it along, all data will be lost and can't rehabilitate.

2. Damage to or destruction of data or code inside or outside the system

Your data is altered, destroyed or stolen by outsiders with their device or your own device via code snippets.

Figure 2: Damage to or destruction of data or code inside or outside the system

Example: Mobile game maker Zynga announced that a hacker had stolen account login details on September 12 for customers using its popular games including "Draw Something" and "Words with Friends". In addition to login information, hackers also stole usernames, email addresses, login IDs, some Facebook IDs, phone numbers and Zynga account IDs of about 218 million customers who installed the game version on iOS and Android before September 2019 to do something against the law **[1]**.

3. Damage to or destruction of physical system assets and environment

Hardware irreversibly damaged or you have a technical problem causing the HATA in the hardware to disappear.

Example: Suppose you are making an assignment and you accidentally spill water on your computer make for it power off while you not yet save that data, so your data cannot be restored. This is due to the external environment affecting your data.

Figure 3: Damage to or destruction of physical system assets and environment

4. Unauthorized removal or copying of data or code from a system

Someone will used unauthorized software to get your information.

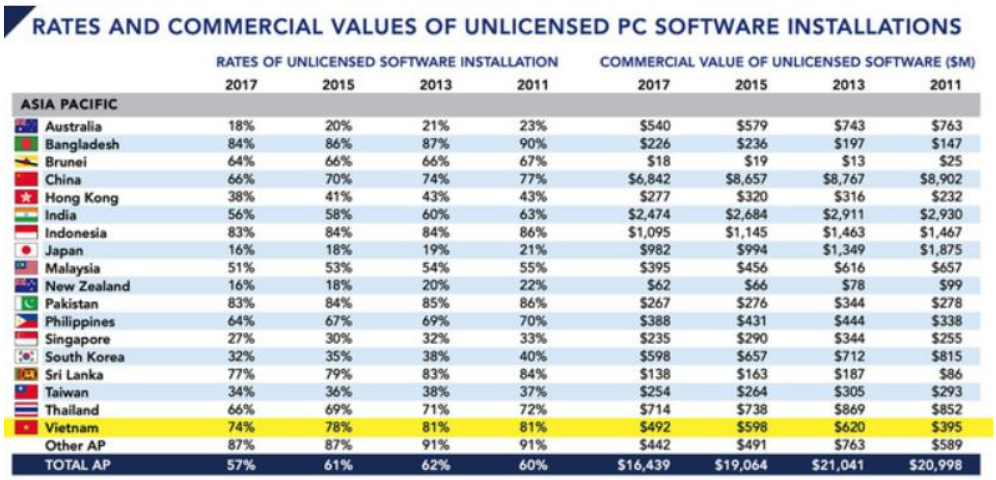
Figure 4: Unauthorized removal or copying of data or code from a system

Example: You use third party software such as malicious code, worms, viruses, etc.., as malware on data to blackmail someone.

5. Unauthorized use of the software

Someone uses unauthorized software to access database data to get information from those facilities.

Example: You use unauthorized software to read stories and you need to log in with your personal information. Your information is then at risk of being stolen through malware that is often hidden in the unauthorized software you are using.



RATES AND COMMERCIAL VALUES OF UNLICENSED PC SOFTWARE INSTALLATIONS

	RATES OF UNLICENSED SOFTWARE INSTALLATION				COMMERCIAL VALUE OF UNLICENSED SOFTWARE ($M)			
	2017	2015	2013	2011	2017	2015	2013	2011
ASIA PACIFIC								
Australia	18%	20%	21%	23%	$540	$579	$743	$763
Bangladesh	84%	86%	87%	90%	$226	$236	$197	$147
Brunei	64%	66%	66%	67%	$18	$19	$13	$25
China	66%	70%	74%	77%	$6,842	$8,657	$8,767	$8,902
Hong Kong	38%	41%	43%	43%	$277	$320	$316	$232
India	56%	58%	60%	63%	$2,474	$2,684	$2,911	$2,930
Indonesia	83%	84%	84%	86%	$1,095	$1,145	$1,463	$1,467
Japan	16%	18%	19%	21%	$982	$994	$1,349	$1,875
Malaysia	51%	53%	54%	55%	$395	$456	$616	$657
New Zealand	16%	18%	20%	22%	$62	$66	$78	$99
Pakistan	83%	84%	85%	86%	$267	$276	$344	$278
Philippines	64%	67%	69%	70%	$388	$431	$444	$338
Singapore	27%	30%	32%	33%	$235	$290	$344	$255
South Korea	32%	35%	38%	40%	$598	$657	$712	$815
Sri Lanka	77%	79%	83%	84%	$138	$163	$187	$86
Taiwan	34%	36%	38%	37%	$254	$264	$305	$293
Thailand	66%	69%	71%	72%	$714	$738	$869	$852
Vietnam	74%	78%	81%	81%	$492	$598	$620	$395
Other AP	87%	87%	91%	91%	$442	$491	$763	$589
TOTAL AP	57%	61%	62%	60%	$16,439	$19,064	$21,041	$20,998

Figure 5: Unauthorized use of the software: Table of statistics about the incidence of illegal software usage and their value in Asia-Pacific countries **[2]**

6. Solutions to organizations.

- ✓ There are reasonable security measures in place
- ✓ Use anti-virus software
- ✓ Use the authentication method
- ✓ Use intrusion detection / prevention system
- ✓ Update of new operating system for system
- ✓ Use fire detectors and automatic fire fighting without using water to put out the fire
- ✓ Use voltage controller
- ✓ Use air conditioning to control humidity
- ✓ Use password procedure
- ✓ Use the right data security procedure for all data

P2 Describe organizational security procedures

"Security procedure" means a procedure employed for the purpose of verifying that an electronic signature, record or performance is that of a specific person or for detecting changes or errors in the information in an electronic record **[3]**.

"Security procedure" includes a procedure that requires the use of algorithms or other codes, identifying words or numbers, encryption, or callback or other acknowledgment procedures **[3]**.

1. Password procedure

All authorized users are required to select and maintain a password according to the instructions and request.

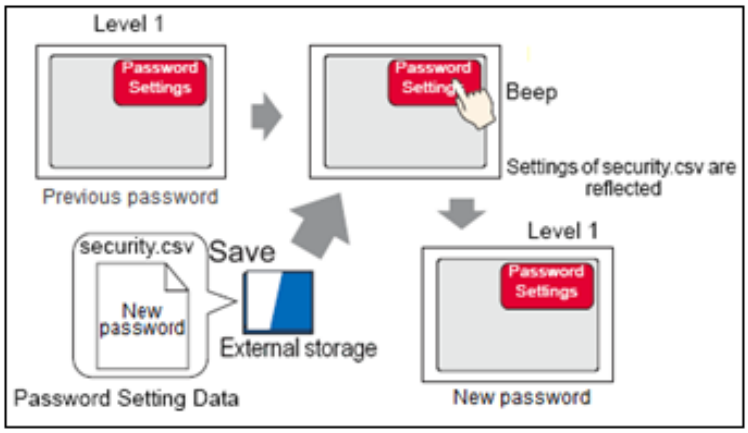


Figure 6: Password procedure

Example: You register a game account and it requires you to set a password for that account with the requirement that the password must be at least 8 characters. There must be enough lowercase letters, uppercase letters, numbers and special characters (*such as*: *realM$N0*).

2. Business continuance

Figure 7: Business continuance

This means to keep going business position and recovering data caused by disasters or incidents involving machines and equipment caused while working.

Example: Assuming your company loses all data due to the explosion, the data cannot be recovered and retrieved because your company only stores those data in computer at company. *Solution*: Create systems such as disk burning, cloud or virtual servers that allow the storage and maintenance of data copies. If a location is disabled, access to this data is uninterrupted. Besides, it also protected against data loss.

3. Anti-virus procedure

This procedure establishes the requirements that must be met by all computers connected to the FIS network to ensure effective virus detection and suppression.

Figure 8: Anti-virus procedure

Solution: Users must not intentionally send or receive, or allow to send or receive any programs or files that they reasonably know or not know to contain any malicious content, including all but not limited to for viruses, worms, trojans or email bombs.

4. Audits

Auditing is defined as the on-site verification activity, such as inspection or examination, of a process or quality system, to ensure compliance to requirements. An audit can apply to an entire organization or might be specific to a function, process, or production step. Some audits have special administrative purposes, such as auditing documents, risk, or performance, or following up on completed corrective actions **[4]**.

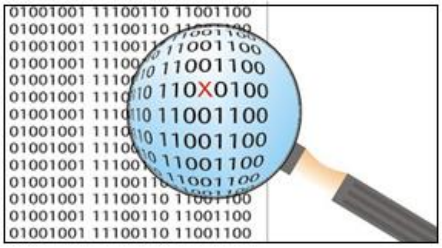


Figure 9: Audits

Example: Suppose your company recently prepared a new product but an hour before its launch, rival of your company, launch products just like your company. Demonstrate the security system of your company's data is not good or have spy in your company. *Solution*: First, the company must check whether the security and data management system are gap or signs of being attacked. If does, system need to be fixed; otherwise, you need to upgrade the entire security system to more layers and install additional control software for the company's common system. Finally, it is necessary to examine the company internally.

5. Backup/restoration of data

Recovery means recovering lost or deleted data, but the ability and quality after restoration depends on the level of previous damage. Backup means copying and storing data to available storage ports like Cloud, Microsoft, etc.

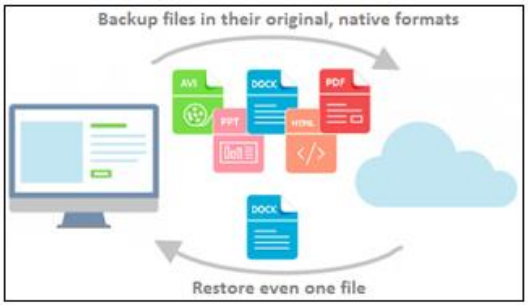


Figure 10: Backup/restoration of data

Example: Assuming your computer memory is full, you cannot delete any data from the device to store new data. Solution: back up data to Cloud, Microsoft, etc., to optimize the amount of memory in your computer memory. This gives you more space in your storage, avoids data loss, and increases your computer's lifespan.

M1 Propose a method to assess and treat IT security risks

1. Security risks assessment

Is finding about out what risks apply to your business and assessing them. Management must decide what risks will be treated or not. Also, can be interpreted as creating a snapshot of current risks. More technically, it covers the following stages: *Identifying threats* (identifying all relevant threats); *Threat characteristics* (determining the impact and capabilities of associated threats); *Exposure assessment* (identify asset gaps); *Risk characteristics* (identify risks and assess their impact on businesses) **[10]**.

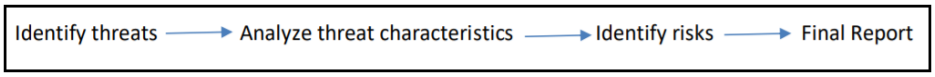


Figure 11: Steps to assess business security risks

Example: Assuming your company needs to look at the overall app portfolio from an attacker's perspective to prevent security breaches and security hole then the evaluation should be done. This helps your company make decisions about allocating resources, tools and security control correctly and safe more.

2. Security risks treatment

Is selecting and implementing security controls to minimize risks. Control may have different effects **[10]**. The process for this job is as follows: *Identification of Options* > *Development of Action Plan* > *Approval of Action Plan* > *Implementation of Action Plan* > *Identification of Residual Risks*. You can handle risks in many ways. However, it is necessary to calculate and devise the most appropriate method because it is the key to optimize performance and minimize risk.

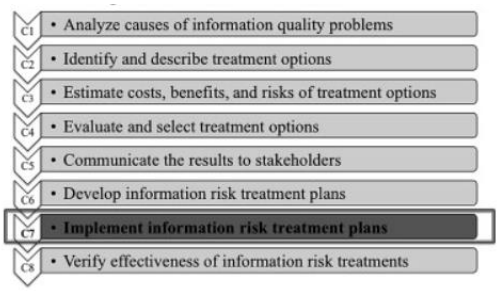


Figure 12: Security risks treatment

Example: Assuming that after your company has identified the potential risks of data loss, it is necessary to devise the most appropriate and optimal plan to handle this risk right away. When there is plan, begin proceed eliminate the risks. Once completed, check to see if all the old risks have been removed and if there are any new risks. Finally, it is possible to upgrade the system to make sure more secure before.

LO2 Describe IT security solutions

P3 Identify the potential impact to IT security of incorrect configuration of firewall policies and third-party VPNs.

1. Firewall policies

1.1. Overview of a firewall

Network firewalls can be hardware or software, or a combination of both that is used to reduce or eliminate the occurrence of unwanted network communications while allowing all legitimate communication to flow freely. In most server infrastructures, firewalls provide an essential layer of security that, combined with other measures, prevent attackers from accessing your servers in malicious ways **[5][6]**.

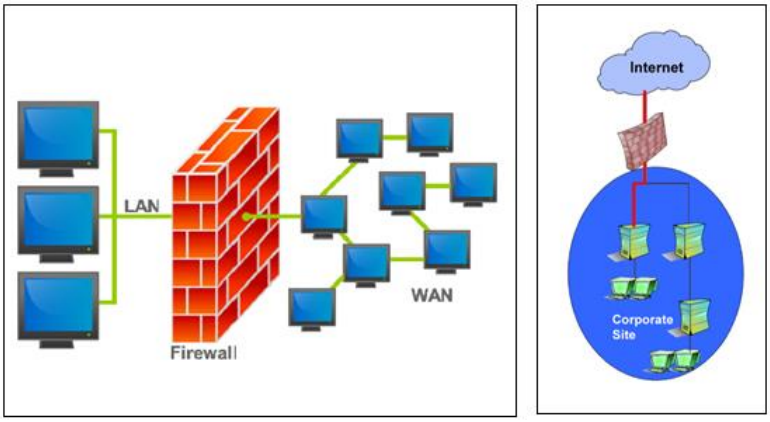


Figure 13: Overview of a firewall

Example: Assuming you're watching a movie on website and accidentally clicking on an ad link that may contain malware or is infected with a virus, the firewall software in your computer will prevent malicious software or viruses from wanting to hacking into your computer.

The potential impact (Potential Threat) of incorrect FIREWALL and IDS configuration on the network is in the configuration. You will be misconfiguring so an attacker can access vulnerabilities in the service so they can access and retrieve your personal data.

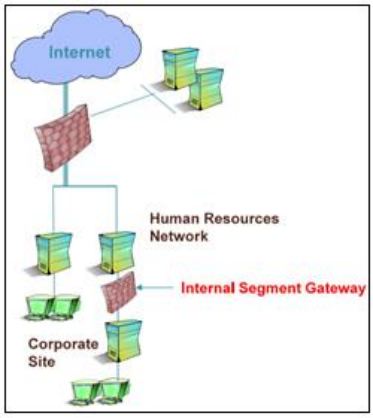


Figure 14: Diagrams the example of how firewall works

1.2. Intrusion Detection System (IDS)

Intrusion: a set of actions aimed at compromising the security goals (confidentiality, integrity, availability of a computing / networking resource) **[5]**.

Intrusion detection: the process of identifying and responding to intrusion activities **[5]**.

IDS: system that performs automatically the process of intrusion detection **[5]**.

Intrusion Detection Approaches **[5]**:

Modeling

- *Features*: evidences extracted from audit data
- *Analysis approach*: piecing the evidences together
  - Misuse detection (a.k.a. signature-based)
  - Anomaly detection (a.k.a. statistical-based)

Deployment

- *Network based*: monitor network traffic
- *Host based*: monitor computer processes

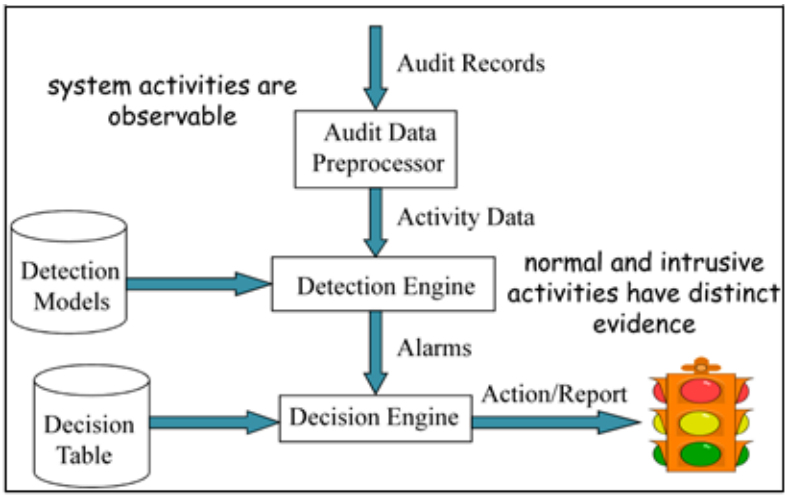


Figure 15: Components of Intrusion Detection System (IDS)

2. Third-party VPNS

Third-party VPN providers often do not provide the same level of security as what you would get if you operating it yourself, your data will not be encrypted when leaving the VPN provider's server except when the server or website you last connected to uses an encrypted connection. This is useful if you want to keep eavesdroppers from snooping on while you're on Wi-Fi, but if you want end-to-end encryption, you should to set up your own VPN system **[7]**.

Example: Assuming that you are assigned to log in and get someone's information available on your computer, you may unintentionally disclose that person's account information to others causing data loss.

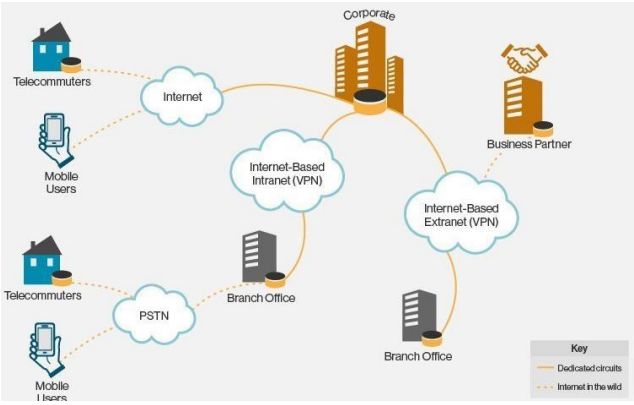


Figure 16: Third-party VPNS

P4 Show, using an example for each, how implementing a DMZ, static IP and NAT in a network can improve Network Security.

1. DMZ

DMZ is known as a neutral network between intranet and Internet. This is the most essential information container, allowing users from the internet to access and accept attacks from the internet **[8]**. DMZ contains many risks in information technology field, these risks come from external factors. We can put a firewall between the DMZ and the outside network. It will control the connection from the external network to the DMZ. On the local network and DMZ, we can set another firewall to control traffic from the DMZ to the intranet.

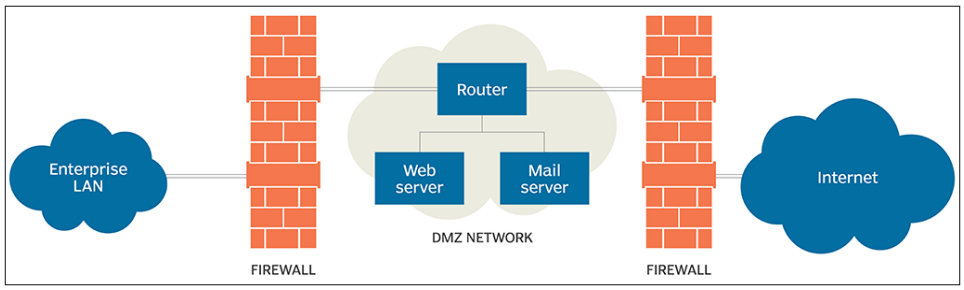


Figure 17: DMZ network architecture

Example: Suppose you want to access a certain website provided that the servers have to be arranged in the technical department and the DMZ portal must allow data packets to pass through. The portal will then check that you are eligible to access this site, if approved, you will be able to access it and vice versa. This helps the data in your server more secure.

2. Static IP

It is called static because it can't change. Is the IP address manually configured for devices. Security is another weakness when using static IP addresses. The never changing address gives hackers a long time to look for vulnerabilities in the device's network **[9]**.

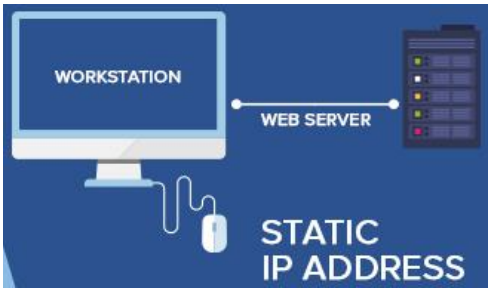


Figure 18: Static IP

Example: Suppose your company uses static addresses. Computers connected to a file server on the network can be to always connect to the server instead of its name. Even if the DNS server is down, computers can still access the file server because they will contact the file server directly via IP address.

3. NAT

Converts a network's illegal IP addresses to legal or public IP addresses. Mean, hides the true addresses of individual hosts, protecting them from attack and allows more devices to be connected to the network **[5]**.

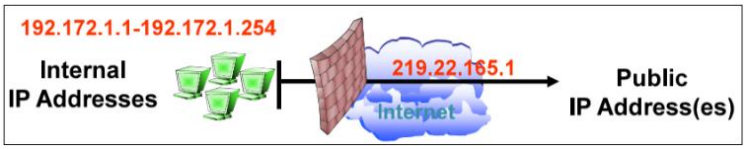


Figure 19: Network Address Translation (NAT)

Example: Assuming you want to access a network device, you need to connect to it. The NAT in that network device will then convert your IP into a public IP (*private IP: **192.172.1.3**> **219.22.165.1** public IP*). This helps keep your device secure.

M2 Discuss three benefits to implement network monitoring systems with supporting reasons.

1. Some of the networking monitoring devices

- ✓ Security information and event management (SIEM)
- ✓ Solar-winds Network Performance Monitor
- ✓ ManageEngine Op-Manager

2. Why do you need to monitor network?

Because, it helps monitor the usage and performance of your computer network and checks for slow or defective systems. The system will then notify the network administrator of any performance issues or outages with some kind of an alarm or an email. This system will save a lot of money and reduce many problems. That is the best way possible to ensure that your business is functioning properly **[11]**.

3. The three benefits of a monitoring system (SIEM)

Centralized management: Each terminal needs to have a system to record security events and regularly transfer this log data to the SIEM server. An SIEM server receives log data from different devices and then performs statistics, analysis, and reporting to create a unique report that shows the correlation between device security events **[5][10]**.

Figure 20: Centralized management

Monitoring network safety: show different parts of the attacks through multiple devices and then reconfigure the sequence of events and determine what the original attack was and whether it will succeed or not. Mean check the log data of all these events and determine if the target server has been infected or attacked successfully, so it can isolate them from private network and handle the attack work **[5][10]**.

Improve efficiency in troubleshooting activities: means that troubleshooting efficiency is significantly increased, it helps saving time and resources for troubleshooting staff. Besides, it also provides a simple interface to review all security log data from multiple terminals **[5][10]**.

LO1 & 2

D1 Investigate how a 'trusted network' may be part of an IT security solution.

A trusted network is a network of connected devices, open to authorized users, and allows for only secure data to be transmitted. From this, it can be said that reliable network is also a solution in IT security.

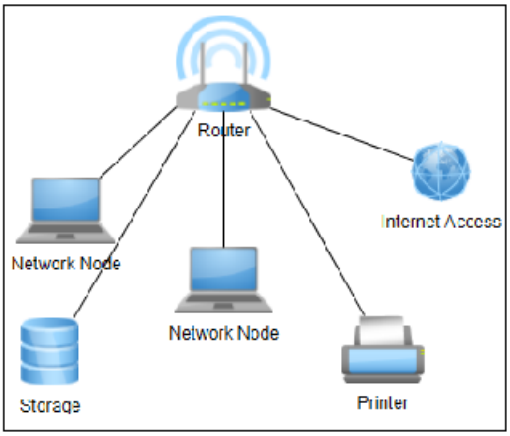


Figure 21: Trusted network

Example: Suppose, when you use a registered network, If someone wants to access this network, they need authorization. If that person has been authorized, the data that he or she wants to transmit needs to be confidential.

Conclusion

For effective information security, first identify the risks that may be encountered. The second is to use solutions to reduce the adverse effects on the business activities of each security breach. Note, when using security solutions such as firewalls, VPNs, etc., care should be taken when configuring because misconfiguration can affect security quality. Finally, evaluate and handle all security related issues.

Evaluation

The information contained in the report and the research results is reliable because it is referenced from books, lecture slides and reputable websites. Besides, there are still some content that is evaluated in my opinion, it is viewed from an objective perspective and my level of understanding so there will be some not quite accurate.

References

[1] TapChiTaiChinh. 2020. *Điểm Lại 5 Vụ Đánh Cắp Dữ Liệu Lớn Nhất Năm 2019*. [online] Available at: <http://tapchitaichinh.vn/tai-chinh-quoc-te/diem-lai-5-vu-danh-cap-du-lieu-lon-nhat-nam-2019-316913.html> [Accessed 19 April 2020].

[2] Cafebiz.vn. 2020. *Việt Nam Có Tới 74% Phần Mềm Đang Sử Dụng Là Trái Phép, Tỷ Lệ Cao Nhất Nhì Đông Nam Á*. [online] Available at: <https://cafebiz.vn/viet-nam-co-toi-74-phan-mem-dang-su-dung-la-trai-phep-ty-le-cao-nhat-nhi-dong-nam-a-20191023165104546.chn> [Accessed 19 April 2020].

[3] Oregonlaws.org. 2020. *Definition Of Security Procedure - Oregon Legal Glossary*. [online] Available at: <https://www.oregonlaws.org/glossary/definition/security_procedure> [Accessed 20 April 2020].

[4] Asq.org. 2020. *What Is An Audit? - Types Of Audits & Auditing Certification | ASQ*. [online] Available at: <https://asq.org/quality-resources/auditing> [Accessed 20 April 2020].

[5] 2020. *Network Security Term Firewall VPN IDS IPS SIEM_For ASM1*. [ebook] Available at: <https://classroom.google.com/u/1/w/NjUyNzkxNjQ4MDFa/t/all> [Accessed 21 April 2020].

[6] Digitalocean.com. 2020. *What Is A Firewall And How Does It Work? | Digitalocean*. [online] Available at: <https://www.digitalocean.com/community/tutorials/what-is-a-firewall-and-how-does-it-work> [Accessed 20 April 2020].

[7] Techsoup.org. 2020. [online] Available at: <https://www.techsoup.org/support/articles-and-how-tos/everything-you-need-to-know-about-vpns> [Accessed 20 April 2020].

[8] Công Nghệ Hà Nội. 2020. *DMZ Là Gì? Những Thông Tin Cơ Bản Và Đầy Đủ Nhất Về DMZ*. [online] Available at: <http://congnghehanoi.edu.vn/dmz-la-gi.html> [Accessed 20 April 2020].

[9] Quantrimang.com. 2020. *Địa Chỉ IP Tĩnh Là Gì?*. [online] Available at: <https://quantrimang.com/dia-chi-ip-tinh-la-gi-160105> [Accessed 20 April 2020].

[10] 2020. *Risk Assessment And Risk Management Methods: Information Packages For Small And Medium Sized Enterprises (Smes)*. [ebook] Available at: <https://www.enisa.europa.eu/publications/information-packages-for-small-and-medium-sized-enterprises-smes/at_download/fullReport> [Accessed 21 April 2020].

[11] Blanchard, C., Blanchard, C. and Monitoring, T., 2020. *The Importance Of Network Monitoring*. [online] i.t.NOW. Available at: <https://itnow.net/the-importance-of-network-monitoring/> [Accessed 21 April 2020].