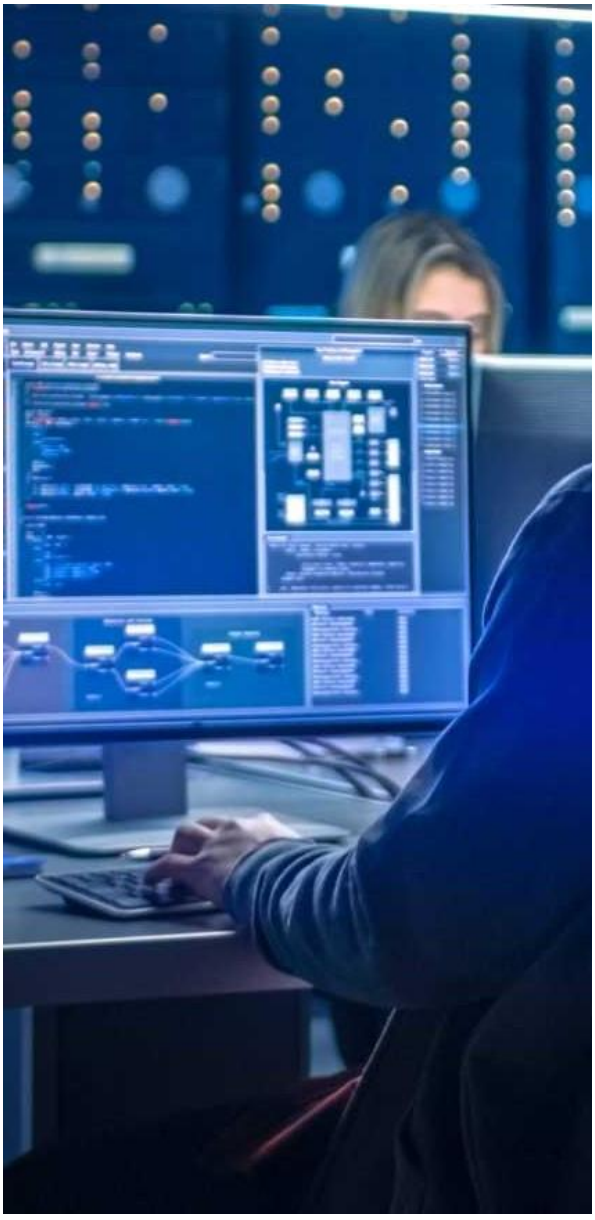


COURSE WORK

16/4/2022

STUDENT NAME
Ali Mohamed Abdelhamid

Student ID
202100274

Table of Contents

Executive Summary / Abstract

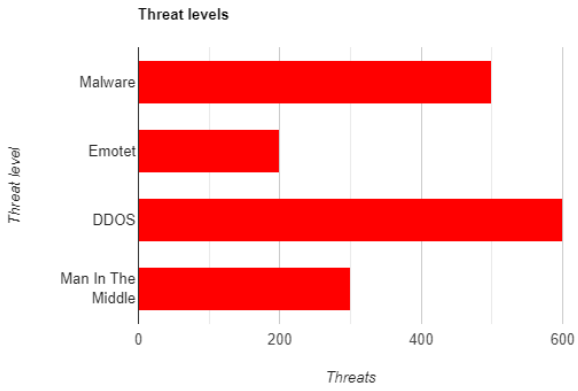
myFinTech is a famous financial advisory startup, which wants to revamp its security system to provide a secure and uninterrupted service to its customers. These secure services are hosted in their main headquarters/ main data center. Their current network setup consists of the following devices: 17 Computer devices, 2 Access points, 1 Switch, 1 Firewall, 1 Web Application Server, and 1 Router. In this essay, I shall report all my recommendations and revisions that the company should apply; By identifying the flaws in the infrastructure and current active systems, then separating them according to their level of severity. I will then proceed to produce a plan that will help mitigate and in the best-case scenario eliminate the threat, furthermore, I will construct a new security policy that will cover all the IT components and infrastructure, while taking into consideration the awareness security development.

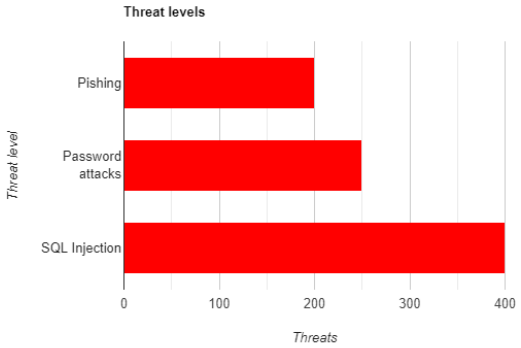
Identify Security Posture

A security posture consists of multiple things, including: 1- the level of automation present in your security infrastructure, 2- the controls and processes that are set in order to secure your enterprise against cyber-attacks, 3- the level of transparency that is present in order to view your inventory and attack surface, 4-your limitations to detect and prevent attacks, 5- and the ability to recover and react from security breaches.

Revise the current security posture and identify the flaws in the current system and infrastructure

How can you evaluate the current security posture? The security posture assessment is the very first step in understanding where you are currently in the security level hierarchy; but in order to actually revise it, multiple questions need to be asked: How secure is the organization?, How good are our security controls?, Do we have the right cyber security strategy?, and many more, however, in our current analysis. The current organization is secure, it is clearly open for some improvements that will increase its security level and allow them to provide a much reliable service to their customers. The currently placed cybersecurity strategy is considered good, since they're taking into consideration multiple security flaws and their mitigations, they are also taking into consideration all the possible backdoors, and weak points that have been discovered in the past, as well as automating the process since attackers are working 24/7 looking for vulnerabilities, a study shows that hackers have found over 100 vulnerabilities in a single month. Furthermore, you cannot fully measure the cyber-resilience of a security system unless you have a full force of penetrators ready to start breaching the system from every angle, however, you can measure the breach risk and order them based on the threat level:

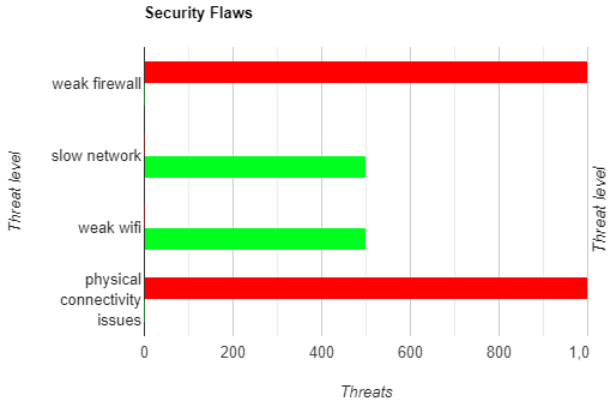


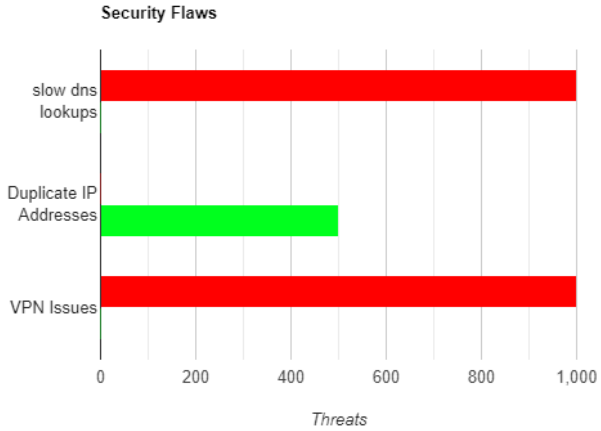


The vulnerability management program is not the best there is, there is a lot of improvements that can happen that will greatly improve their service, they have a high risk against all internet-based attacks such as: SQL Injection, DDOS attacks, as well as Malware attacks, this is highly due to the weak firewall and the weak internet security system that is set. As seen in the two figures above, I have used a bar graph to mark the hierarchy levels of the threats, this will allow the company to view the scoreboard and then benchmark the different risks. Furthermore, the best way to discuss the company's future towards the cybersecurity improvements as well as the organizations security posture, is through a thorough detailed report including all the threats and the mitigation plans.

Plan to mitigate the security flaws

I have discovered many security flaws and issues that are present in the cyber system and have categorized them as high threat and low threat, the flaws found were a weak security system, a slow network, a weak wi-fi signal, physical connectivity issues, slow DNS lookups, static and duplicate IP addresses, and VPN issues. There are actions that could be made to mitigate such issues, first, let's start with the high-risk flaws; start by purchasing a new firewall system and device, it could be costly, but it will be of great benefit, next, the physical connectivity issues, the entire network can break up just due to one cable being cut or damaged, this is not practical and will result in bad service delivery. Next, is the slow DNS lookups, how DNS works is by hopping over multiple servers while matching the DNS cache and repeating the process, if the lookup for the cache is slow this will cause a slow link and might even cause an overloaded server, to fix this issue, the local network administrator could set the DNS to shift to route through faster chain servers. Furthermore, the low-risk issues, first a slow network, this would usually not cause many issues except the fact that both employees and customers will have a bad experience with your service, the employees will have a slower workflow and therefore deliver a slower service to the customers, the best solution to this is to contact your ISP and order a higher speed and larger quota package. On the other hand, duplicate IP addresses, since no 2 computers can have the same IP, any instance where that happens the system will be completely unreliable, and it will lead to a network failure of operation, this will also limit the allowed number of devices on the network to seventeen since the IP range present is from 0/16.





Security Policy

A security policy contains many responsibilities, not just on the employee, but also the company itself. The following is the recommended company security policy:

The scope of this security policy covers the transmission, storage, access, and destruction of information. Therefore, it logically applies to the code of conduct of the staff, workers, and others who have access to confidential information, as well as the systems, applications, process, transmit, host, and store information, whether on-site, personal or company owned. The enforcement of the security policy is the duty of the manager of resources, the resource manager will report to the security access manager with the login credentials and information of the user that is requesting the information, the information reported should include, the type of data requested, the name of the user, the date, and the reason behind the request.

1. *Objectives*
    - Promote a clean approach to the management of information security
    - Build an 'aware' community that is careful with the security and privacy of information
    - Protect the companies private and uncleared information against the compromise of its confidentiality.
2. *Workers*
    - Workers are required to protect and are responsible to keep the company's information and technology systems safe, and to maintain such policy and regulate the framework, if any workers suspect or discovers any breach of information or material, they shall report to the DPO located at their office or through their email. Workers shall also accept that they are fully responsible while using the company's facilities and machines and will indeed take all the required steps to protect the company's information.
3. *Vulnerability Management*
    - Application-layer penetration tests
    - Network-layer/infrastructure penetration tests
    - Internal and external vulnerability tests quarter yearly
    - Static code testing
    - Manual testing after any significant network changes
    - Testing of the product environment
    - Dynamic code testing
    - Reporting of any finding in a timely manner
4. *Password Policy*
    - Requirements when creating a password relating anything to the company and anything that contains confidential information:
    - A minimum of eight characters
    - Must contain uppercase characters
    - Must contain lowercase characters
    - Must contain a digit
    - The usage of symbols is highly recommended although optional
    - Password must be modified after every 90-day period
    - Must not include the user ID
    - Must not be common or easily guessed
    - User account will be locked after 7 or more failed attempts

- Lock duration will last for 30 minutes and will increase accordingly
- User session will lock after 5 minutes of inactivity and will result in re-entering the password

5. *Messaging security*
    - Outgoing emails should be setup with the data loss prevention monitoring
    - All incoming emails should be scanned for Phishing, Viruses, and Spam
6. *Anti-Virus*
    - The IT department shall implement network controls that should enable the usage of company provided firewalls that will then be used to scan for intrusion attacks and detect system traffic
    - Any files the users may download shall be scanned for viruses as part of any download process for protection purposes
    - The security staff shall ensure the anti-virus applications and security system are up-to-date and are always working properly.
7. *General software rules*
    - All applications that would be installed are the responsibility of the IT department, Users are therefore not allowed to install any type of software without the review of the IT department first.
    - All applications that are already installed should always be kept up to date to verify the integrity of their security flaws

POLICY VIOLATION PROCEDURE:

In the event of the discovery of a worker/ staff violating any of the reported policies will be legally subject to the company's set disciplinary procedures, and will be reported to the relevant law institution, due to the varying damage that may be done by the different violations the company will act based on every case solely.

Recommendations

As mentioned above the low threat issues are as follows: Slow network, slow Wi-fi, and duplicate IP addresses. I have also mentioned in the previous paragraphs what should be done to prevent and mitigate these issues, but as a restatement, A slow network might cause many issues, the slow delivery of the service, therefore customers will not have the quality of service. A slow network may also cause the issue of slow information delivery, for example, a security breach has been made, for the discoverer to tell the security manager he needs an adequate internet speed to reach him as fast as possible. The slow wi-fi issue will also foundationally lead to the same issue as the slow network. On the other hand, the physical connectivity issues, are that if a cable was cut during any type of physical labor, the entire network could fail, therefore, some precautions should be made, multiple data centers should be made, as well as a backup generator that would replace the power source if the power went out for any type of reason.

Planning & Budget Estimation

The company needs to start with setting up a stronger security system, I recommend the Fortinet FG-200E, due to its high reliability and excellent protection, it would be the most fit candidate to the company, however it may be a little costly with a 65,000EGP price tag. Next the company could next get the backup generator I mentioned above, the one I would suggest is Easy UPS 1Ph on-line SRVS with a 10000VA and 230V which is the same as a wall outlet, this generator would act as a safeguard for when the power goes out no information would be lost, this costs around 49,200EGP, next you could subscribe to a premium high-end DNS service, my recommendation would be Cloudflare, this would cost the company about 3700EGP monthly, which would account to 44,500EGP yearly, in order to fix the slow internet/ network issue, I would recommend contacting an external ISP that has a good reputation, such as AT&T, their pricing is as listed 3,400EGP monthly and a 40,800EGP yearly but for a 5 gigabyte speed upload and download simultaneously, this would provide a fast internet that is capable of doing any task without ever hindering the working force. The total cost would come out to about 114,220EGP as a one-time cost and an 85,300EGP yearly.

I was not able to provide a Gantt Budget chart.

Conclusion

In conclusion, the company's current security system is good but is open to a lot of suggestions and improvements, it is victim to a lot of threats, as mentioned above, there are some threats that are high threat while some have low threat level, if the company is ready to spend to money, they could improve their systems and deliver a safer and faster secure service to their customers. The security is also present for the employees to read and for the CEO to approve of.

Appendix A: Vulnerability Flaws and Mitigation

Risk Rating Scale

Low, Medium, High

Default or Weak Credentials

Rating: High High/Medium/Low

Description: Weak Firewall

Impact: Would cause the system to be easily penetrated and loss of credentials and crucial information.

Remediation: The purchase of a stronger security system device and a cleaner set up with safer precaution and software.

Rating: Low High/Medium/Low

Description: Slow Network

Impact: Slow transfer of information and slow service delivery

Remediation: Contact a new ISP and subscribe to a stronger internet package

Rating: Medium High/Medium/Low

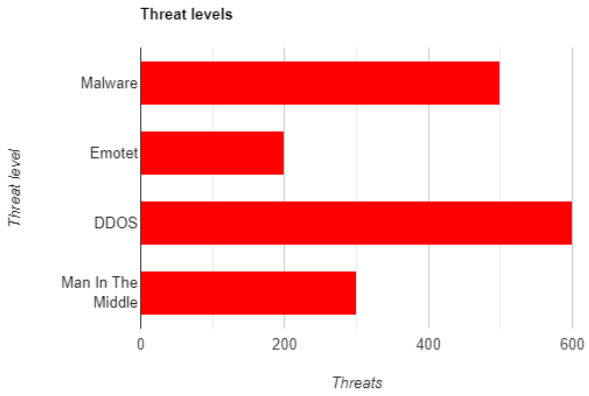
Description: Physical Connectivity Issues

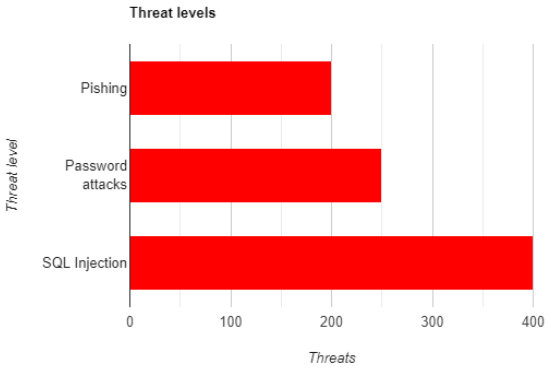
Impact:	Would cause loss of information in the event of power loss and even a penetrator could slip through while the system is booting up
Remediation:	The purchase of a backup power generator to prevent the shutting down of any system due a physical malfunction
Rating: High **Description: Slow DNS Lookup**	**High/Medium/Low**
Impact:	Would cause a slow data transfer between data centers due to the slow lookup of the DNS server
Remediation:	Subscribe to a higher end DNS provider host
Rating: Medium **Description: Duplicate IPs**	**High/Medium/Low**
Impact:	Would cause an entire network malfunction and might cause a network shutdown

Remediation:	A cleaner setup of the network with a limited number of Ips depending on the number of devices present on the network.

Rating: High	**High/Medium/Low**
Description: VPN Issues	
Impact:	Could cause slippage of information due to the weak security of the VPN and cause an attack called Man-in-the-middle, these attacks would cause the attacker to intercept all data going from and to the network
Remediation:	Subscribe to a high-end VPN service provider, usually they would be the same provider as the DNS.

List of Tables





References

1. *Bar Graph Maker | create a bar chart online - rapidtables.com*. (n.d.). Retrieved April 18, 2022, from https://www.rapidtables.com/tools/bar-graph.html

2. Edwards, F. (2021, January 5). *Its security policy template*. Free Privacy Policy. Retrieved April 18, 2022, from https://www.freeprivacypolicy.com/blog/it-security-policy-template/

3. *FortiGate 200e Price & Datasheet - Fortinet FG-200E*. (n.d.). Retrieved April 18, 2022, from https://www.router-switch.com/fg-200e.html

4. Jacobs, D. (2022, January 26). *Nine most common network issues and how to solve them*. Search Networking. Retrieved April 18, 2022, from https://www.techtarget.com/searchnetworking/answer/What-are-the-3-most-common-network-issues-to-troubleshoot

5. *Our plans: Pricing*. Cloudflare. (n.d.). Retrieved April 18, 2022, from https://www.cloudflare.com/plans/#faqs

6. *Power shop*. Power Shop. (n.d.). Retrieved April 18, 2022, from https://powershopeg.com/ar_EG/collection/product/SRVS10KI?variantCode=SRVS10KI&gclid=Cj0KCQjwmPSSBhCNARIsAH3cYgZXc2b8u0Wraja9kYjexa3Kg8F6DxhgfWa2BOdMXzEt0k9LJZTsppwaAiHyEALw_wcB