Computer science

I am hired as Information Security Officer for a pharmacy. I have identified and analyzed physical and logical access controls in network to protect medication and funds maintained located on the premises and data protection. I was notified that malicious activities are taking place in the network structure. In this paper I have identified potential, physical and logical vulnerabilities in the pharmacy networks. I have described the potential impact of all malicious attacks & threats and identified vulnerabilities to the network and the organization. Security weaknesses are analyzed in details. Then I have proposed a plan to deal with security issues and vulnerabilities. I am assigned to resolve these issues that arises in the network structure. In this document I will analyze and assess potential malicious attacks and threats that may be carried out against the network along with potential vulnerabilities that may exist in the documented network.

Vulnerabilities are weak spots in the network systems that allows the hackers to exploit into the network system. The attacker access the flaw in the system, enter through that hole and do whatever he want. He can use different tools to identify those weak spots that require little or no hacking knowledge to implement, applications intended for troubleshooting and maintaining and optimizing networks. There are different risks associated with vulnerabilities: data loss, down time, network busy, and shutdown of the network. There are different Vulnerabilities types: Technology weaknesses, Configuration weaknesses, Security policy weaknesses. Technology weaknesses includes TCP/IP protocol weaknesses, operating system weaknesses, and network equipment weaknesses.

Network equipment weaknesses includes Password protection, Lack of authentication and

Routing protocols. Operating system weaknesses includes operating system vulnerabilities like not updating the operating system. Configuration weaknesses include unsecured user accounts, System accounts with easily guessed passwords, Misconfigured Internet services, unsecured default settings of the software products, and misconfigured network equipment’s. Security Policy Weaknesses include lack of written security policy, poorly chosen or default passwords, inadequate monitoring and auditing, unapproved applications installation (Rufi, 2007). Mail Servers are other targets in which hackers want to gain access to network resources. Companies that access e­mail from the Internet, especially, are potential targets (Rampat). Threat can be performed to the network when attackers take advantage of the vulnerabilities and it has a negative impact on the network.

I have assigned to identify and analyze potential vulnerabilities in the pharmacy network. In pharmacy network there can occur network security weaknesses. Hackers can attack different protocols like HTTP (Hyper Text Transfer Protocol), FTP (File Transfer

Protocol), ICMP (Internet Control Message Protocol) which are inherently insecure.

There may be operating systems weaknesses in the pharmacy network like in Win 7 or Windows Server 2008. Unmanaged Network equipment can cause security hole in the network to invite hackers to attack in the system. Unmanaged routers, firewalls and switches can cause weaknesses. These weaknesses are related to password protection, device authentication, routing protocols and firewall holes. Also administrators or network engineers who do not know the network configurations properly can cause weaknesses in the network. Incorrect configuration of network devices or security software or firewall devices can help to compromise a network. Others vulnerabilities can be unsecured employee and user accounts information or passwords, system accounts information or passwords, misconfigured internet services, unsecured default settings within products, misconfigured network equipment – ACLs or routing protocols.(1) If pharmacy employees do not follow the security policy for accessing pharmacy data, then security weaknesses can occur. Different network threats can be resulted due to these potential vulnerabilities in the network. Hackers can make use of tools, shell scripts or SQL injections to attack the network. They can be a simple hackers which do not know the domain knowledge of hacking or experienced hackers which know system vulnerabilities. They easily exploit­code and scripts. Some customer or users can make use of network resources and attack networks. They have authorized access to the network. They may be the part of pharmacy. (1)

Physical vulnerabilities are the issues in the network which address the protection of physical security, encompasses both technical and nontechnical components. Physical vulnerabilities are often­overlooked but are the critical aspect of an information security. It covers security weaknesses related to network resources, data centers computers and information. Hackers can exploit a handful of building infrastructure vulnerabilities like they can attack computers, utilities, hardware data center or areas where confidential information is stored. Physical vulnerabilities depend on such factors as size of the pharmacy, number of franchises, Number of employees, location and number of building entrance and exit points, and placement of the data centers. In pharmacy infrastructure, I have identified physical vulnerabilities which may cause serious attack on confidential data. There may not be any receptionist to input visit information, track check each person record visiting pharmacy. There is no any authentication system to allow the entrance restricted people only into sensitive areas of pharmacy. Hackers may make use of different uniforms such as repairers or technicians to enter into sensitive areas. Hackers may pretend as employee and access computers in office to hack data center of pharmacy. IP­based video, access control, and data center management systems are accessible via the network with the default user ID and password. There can be no proper management of company sensitive data files so that hackers easily access them. There can be unsecured desktop computer which are used in pharmacy. (Beaver, 2013)

Logical vulnerabilities in the networks are subjective in nature. Identifying logical vulnerabilities in system cannot be automated. We need to make decisions which require contextual knowledge of the system, plus the ability to "logically" understand any number of previously undefined results. It includes the understanding how could we know that our system is under attacked or we are scammed. How would it know if the attack worked or was adequately defended? We possess a natural ability to assess context in which different network issues arises. These issues can be only identified by humans. Using intelligence unique to humans, we can quickly deduce their purpose with relative certainty. Logical vulnerabilities depends upon firewall, security passwords strength, security software, data centers authentication, network security. Let us discuss the logical vulnerabilities that may arise in the given network architecture. Hackers can attack globally to find security holes in pharmacy network. They can break firewalls and steal pharmacy important data or destroy it. They can exploit system to intrude viruses or worms. Hackers can use stealers or key loggers to track different network activities in the data center. Hackers can make use of fake mails or untrusted URLs to attack file servers. They can send fake invoices to buy something. Our pharmacy consultants might use the website for purchasing medicine from untrusted website. The item and price parameter is our topic discussion in this case. The item parameter includes medicine and price parameter includes price for which we are going to pay for a given medicine. Some fraud might be happen here. The price might be changed. If medicine is of $300 it might be changed to $400 or $500. This is the example of logical issue that should also be considered.( Grossman)

Let us analyze and perform risk assessment and risk mitigation, how hackers or intruders identify network potential, physical and logical vulnerabilities to attack the system. In Reconnaissance hackers make use of DoS(Denial of Service) attacks. For example they target pharmacy network to identify different IP of devices or desktop computers that are alive. Then they make use of port scanner to determine what network services or ports are active. Then intruder queries the ports to determine the application type and version, and operating system version. Based on this information, the intruder can determine if a possible vulnerability exists that can be exploited. The hackers or intruders can track all the conversations between peers or customers in the pharmacy networks. This type of vulnerability assessment is called Eavesdropping. Using Network or protocol analyzers and packet capturing utilities, they process queries and gather valuable data on network equipment configuration and crack username and passwords. They can use Trojan horses programs that introduce an inconspicuous backdoor into a host. They can pose themselves as network administrator to gain information from users to access information. They usually look for written usernames and passwords and use brute force, cracking tools and Dictionary attacks to crack easily guessed passwords. Man­in­the­middle attack access vulnerabilities in the network in which hacker have network packets access. He may work for ISP (Internet service provider) and thus have access to all network packets transferred to other networks. ARP spoofing is a wise way to exploit the network. Hackers pretend themselves as a user while talking to pharmacy customer or user. This causes network traffic to pass on the hacker’s system and he can fetch all the information he needed, like username passwords, credit card numbers, and medicine record (Hargrave ). Key loggers and Password stealers like iStealer are famous password cracking tools that are spread over internet. Inexperienced hackers attack system browsers and crack username and passwords which are saved as prompts by browsers. There are other attack methods and software like VNC. (Beaver)The crafty hackers can attack firewalls with the help of insiders which change the rules of the firewalls of desktop computers in pharmacy or simply disable firewalls.(Beaver) By In IP spooling, attacker falsify the source IP address and pretends himself as a customer or employee, enters into system network.(1)

Now let us make a risk control plan which can be used to mitigate the risk regarding to logical vulnerabilities. The first attempt made by hacker for exploiting is reconnaissance. To prevent reconnaissance, avoid providing any useful information to the attacker or untrusted person. The best way is to track scanning attempts to the network and neglect all of them. Port80 Software developed the first Web anti­reconnaissance software solution on the market. To prevent from eavesdropping, pharmacy should implement a policy directive that inhibits the use of protocols with known susceptibilities to

eavesdropping .Using encryption and switched networks forbids eavesdropping. Encryption is used to provide data protection which prevent network form eavesdropping attacks, password cracking, or data manipulation. Man­in­the­middle attacks can be prevented if we track each employee activities. If he try to bypass traffic to untrusted network or person then he should be gripped. ARP spoofing can be avoided if we use VPN (Virtual Private networks) technology and HTTPs which enables SSL layer during network communication. This makes difficult for hackers to view pharmacy network traffic. Avoid malware sites, untrusted certificates or software to prevent hacking Trojans attacking the system. Using trusted internet security bundle and antivirus program prevents attacks of free password stealers, key loggers and other tools which are used by inexperienced hackers. These tools are easily detected by antivirus but can cause real harm if antivirus program is not installed. There is a good convention that do not save passwords in PC files or browsers to prevent data loss incase network is under attack.(1)

To access the risk assessment of physical vulnerabilities; pharmacy infrastructure, utilities, pharmacy office layout & usage, and network equipment & devices are under consideration. Hackers can reach systems if door propped open at night or off times. Gaps under the doors can allow something to enter to trip the sensors. In case of disasters building can be exposed so that looters can gain access to the computers or system. If pharmacy door hinges are outside they can allow hackers to unhook them. Hackers can easily reach the data center if there is no proper alarm system or no monitoring video camera. Hackers can enter into pharmacy premises if there is no proper monitoring of people traffic coming inside and outside of the pharmacy. They can easily attack if there is no protection of confidential information on desk, or packages and mails. Hackers usually search for confidential information in the trash bins or easily access the written network policies in this way. Intruders can easily access pharmacy mail and copy rooms where they can steal mail or company letterhead to use against you .They can also use and abuse fax machine(s). Login credentials of network cameras and digital video recorders (DVRs) can be changed through an external attack or they can disable them and then enter into pharmacy to access systems. These intruders can also enter unlocked computer rooms and mess around with servers, firewalls, and routers.(Beaver)

For preventive control for physical vulnerabilities in building infrastructure, there should be automated doors and thumb detection system locks, windowless walls, and monitoring cameras and alarms. We must consider pharmacy building and data center utilities, such as power, water, generators, and fire suppression, when assessing physical security. These utilities can help fight off such incidents as fire and keep other access controls running during a power loss. These utilities can also be used against employees or customers if an intruder enters the building. We must ensure that major pharmacy utility controls like power or gas systems are placed behind closed and lockable doors or fenced areas out of sight to people passing through or nearby. Security guards should be careful not to allow any person whether employee or customer or visitor to access the controls to turn them on and off. Visitors should be monitored coming inside and going outside the pharmacy. Each employee should have employee card, and customers should be provided with visiting card. Visiting card have stored customer information. It will help customer to enter into the premises where he is allowed. Customer need to expose card to sensor. If customer is allowed to enter door will be opened, otherwise grant would be denied. This is the most critical countermeasure. In this way, untrusted people would not be allowed to enter. Other organizational employees like technicians, labors and cleaners will be allowed to enter unless they have call letter from the pharmacy premises. It should be situated in a crowded area where anybody can see it and no body try to play a trick to enter into it without any reason. Computer rooms and wiring closets should be locked and sensitive areas should be monitored for wrong doings prevention. Data center should have one entering and exit door. Strong cable traps and locks should be used that prevent intruders from unplugging network cables from computers. There should be employee monitoring system that track the activities of each employee in the pharmacy to prevent data intruding. Some employees are not trusted, so they need to be monitored (Beaver).

References

(1)http://www.cisco.com/web/learning/netacad/demos/FNSDemo1\_1/ch1/1\_2\_1/index.ht

ml

Grossman. J. Understanding Technical vs. Logical Vulnerabilities. Retrieve From. http://www.net­security.org/article.php?id=921

Hargrave . V.(2012). What Are Man­in­the­Middle Attacks and How Can I Protect Myself

From Them?. Retrieve.November 28, 2012.From. [http://fearlessweb.trendmicro.com/2012/tips­and­tricks/what­are­man­in­the­middleattacks­and­how­can­i­protect­myself­from­them/](http://fearlessweb.trendmicro.com/2012/tips-and-tricks/what-are-man-in-the-middle-attacks-and-how-can-i-protect-myself-from-them/)

Rampat.A.Vulnerabilities in network systems**.** Retrieved From [**http://searchsecurity.techtarget.com/tip/Vulnerabilities-in-network-systems**](http://searchsecurity.techtarget.com/tip/Vulnerabilities-in-network-systems)

Rufi & Antoon R.(2007) Security 1 and 2 Companion Guide.Dorling Kindersley

Publishing,Inc.South Asia

Beaver.K.(2013)Hacking for Dummies. Pinpointing Physical Vulnerabilities in Your Offic.(p84­p91) John Wiley & Sons, Inc.