Unit 7

Assignment 1 - Know your threats

Daniel Easteal

Contents

Introduction

In this assignment I will be writing up about different security threats that are out there and the impact that these can have on an organization. For this specific assignment I will be writing about the way that aerospace companies can be affected by these security threats and what they can do to the organization. In addition to this I will also be writing about how the companies can help reduce the risk of these security threats from happening and how they reduce the chance they do.

P1 - Explain the impact of different types of threat on an organization

<Look to the leaflet attached at the back of the document.>

M1 - Discuss information security

In this section I will writing about the general threats that can occur to an IT system as well as how the system and the data that it contains can be kept secure and finally some organizational issues that affect the security of the system as well as information security within some systems. This will be a discussion on information security.

Example 1

With this particular issue the impact of the threat is quite high but only to the customers and not to the actual company itself, just indirectly. As mentioned, the main ways that this could happen would be the weakness of the current logins and encryptions. In order for the hackers to gain access to this information, they will first have to gain access to the whole system network that holds this information and this would most likely have to be done remotely. This is where the first security issue will come into play and this is the ability to remote access the system and the security involved within this, this is because the system should not have a very weak connection authentication and should be protected with a very secure password, or even better, and RSA key is length longer than 2048 for optimal security. With this in place the hackers would have to effectively guess a password that is 2040 characters long. In addition to this the airport should also make sure that they us encryption on the database to ensure that if the data is stolen then the actual details cannot be reached and it will take quite a while for the hackers to decrypt the data to a readable format. This will then give the organization time to recover the data or retrieve it from the hackers so that they cannot do anything with it. One example of this was a hacker called Albert Gonzalez who used his hacking ability to steal over 170 million credit cards worth of information that he would then sell on. He did this using SQL injection which utilizes the weak security that some online web pages had and with this he could gain access to the database where the customer information as stored. As a result of this he was caught and placed in jail for 20 years that start in 2010.

Example 2

This threat of staff being dishonest with the system and using it for their own sake would have quite an impact on the IT system and its ability to work correctly. For example, if all the staff had full access to the system then anyone could change it (even accidentally) in such a way that it will not work correctly and this could mean that the system could make mistakes when making bookings or it may break the system completely in such a way that it cannot be fixed easily and this could cause huge problems for the company and lose them a lot of money. In addition to this, the system might contain certain personal customer details that all the staff could have access to, this would therefore mean that the data could be in the hands of the wrong person quite easily. As well as the impact this would have on the IT system this type of internal threat would also have an effect on the organizational issues within the company. One example of an organizational issues within the company would be that with the requirement to have an IT team available to all of the staff within the company due to the way that they will all have different passwords and levels of user access within the system. This will be needed due to the fact that there will inevitably be issues with the system and these will need to be sorted. This will require there to be some additional infrastructure installed in the company like an additional phone line possibly or an additional office somewhere so that there can be help. This is an organizational issue as it affects the management of the whole company and it will also affect the security of the IT system as people could access file they are not supposed to without the different levels of user access being in place. So, this problem can be fixed by making sure that all different users have a secure password and different levels of access to files and folders in the system.

Example 3

With The first example above, the threat to the IT system is very minimal as there is not really anything that has happened to the IT system, but it is still a physical threat that happened to the company and as such the IT systems in place must have failed. This is because there are many IT systems in place like passport control records, wanted lists and ticket scanners that are in place to ensure that only people who are allowed to be on the plane manage to get on and that these people are not dangerous in any way to the plane. In addition to this, if they get on the plane with the intent of hacking the IT system in place there then they might be able to and with this they could spoof certain information about the plane, like its location and status and with this they could get incorrect information from the air-traffic controllers. With this the hackers could put the lives of many people in danger. The other IT threat of physically stealing some hardware from the server will have quite an effect on the whole system that could end up breaking the system as a whole making it unusable at all as it would be missing critical information and could be corrupt making the system unusable to anyone. Alternately the removal of a hard drive could also remove private customer information from a database and if this is not encrypted then the people who stole the hard drives will have full access to the customer information and if that is released then it is not good. In addition to this, you would also want to make sure that you keep the information inside the system secure so that even if the data is stolen then you have ability to know that it will take a who for the people who took the data to find out what it is, this can be done through the use of encryption. Doing this will ensure that the data is secured and that it cannot be stolen, but this can only happen if the data is encrypted with a recent algorithm that uses a very strong password otherwise that data can be read very easily by whoever took it. Finally, making sure that the hardware running the system is kept secure there will need to be additional organizational options set in place so that the IT system has the highest security that it can. The main way that this would happen would be the upkeep of the server room where the servers are stored. This can be done 1 of 2 ways, the first way would be to use an external company to run the software that you need on their servers that are kept secure and private and with the guarantee to fix any hardware problems that you have with the server. Or you can opt to host the software running on your own servers but you will have to make them safe and ensure that they are upkept very well so that there is the minimal amount of downtime possible. The first way has some obvious advantages like all the server work is done for you and the server will defiantly be in a secure room, but it also has some downsides and this is mainly the cost of this as you are paying for that company to keep a server secure and perform maintenance on it whenever it is needed and as they are a business they will need to make money and as such they will charge you more than they actually cost of the services that they provide. However, if you host the server yourself then you will have to make sure they are kept secure and that they are fixed when that is needed and that can take quite a bit of cost, but you will own the server and as such it can be a lot easier to get things with it done.

Example 4

With this type of attack, the effect on the IT system is quite a lot due to the fact that this can completely negate all the necessary data from getting to the server and as such the effect to the IT system is that it effectively shuts it down 100 percent so that it can't do anything useful. In addition to this, there is not a lot of protection that the server can do to stop this as it must assume that all requests that it gets are valid otherwise it would block people who actually need to use the system. In addition to this threat the system going down and not registering people applying for seats on a plane will lose customers from the company as they will see them as being unreliable and as such they might not choose to use that company again and this will mean that they lose money. Furthermore, there is no threat to the data that is stored on the system with this type of attack due to the fact that the attack on the system is only for disabling the system from the outside so it can't affect the system internally so the data will not be as issue here. Finally, there will also be some organizational issues that there will need to be in place in order for the effects of a DDOS attack to be reduced. The main way that the effect of a DDOS attack can be mitigated is through the use of an external DDOS protection site, these work by waiting 5 seconds whenever a user goes to your website before it redirects them. This will then mean that the same user will not be able to send requests to the actual website faster than once per every 5 seconds. This will then mean that the website will not spammed by all of the requests from users and will be operational under a DDOS attack. This will of course require that the company use a third party service for this and this could then mean that there could be some additional issues with the system for the users and it will also have a cost that the airport will have to pay for. This will then require the website to be re-routed through this third party company as well as an additional pay going out that will have to be accounted for.

Conclusion

In conclusion you can see that there are many different ways that a certain company can be attacked in such a way that the data that they hold will be at risk of being compromised or anything else bad happening to it. As mentioned above there are 4 main and different types of attacks that a company such as an airline will have to protect themselves from and these are: external threats, internal threats, physical threats and social engineering threats. Although these threats are very prevalent and can happen a lot you have also seen that there are many different ways that they can be stopped or their effects/effectiveness mitigated.

Bibliography

https://en.wikipedia.org/wiki/Albert_Gonzalez