Aircraft solution essay

Environment, Air

This report is prepared to assist the aircraft solutions (AS), a well-known company for equipment and component fabrication in Southern California, in identifying the most important security vulnerabilities. This report also discusses possible threats, the likelihood of the threats occurring and the threat if exposed in two remarkable areas. Aircraft Solutions maintains a large capacity plant, trained workforce, large variety of equipment, design modules and solution database provided to multiple industries.

These companies include aerospace, electronics and defense sectors. In this report I will focus on the vulnerabilities present in the existing system of Aircraft Solutions and its operations. Company Overview Aircraft Solutions, with its headquarters in San Diego, California develop and fabricate products and services for different companies. It has two divisions, commercial and the defense. The commercial division is in Chula Vista, CA and the defense division is in Santa Ana, CA. They offer designs at low cost and computer aided modeling packages.

They also provide lifecycle of the product being manufactured. Security Weakness In the two key areas targeted, I will discuss here about the vulnerabilities in hardware and the software. Hardware Vulnerabilities In my security assessment on the hardware of AS, it has been identified that it’s hardware system could be a potential security weakness and cause a threat in the near future. Their system has; 1. Five individual servers 2. A switch 3. Two routers 4. A firewall In this hardware design, there are two main problems.

1. Lack of adequate protection between its commercial division and the rest because of the absence of an extra firewall. 2. DD Santa Ana has direct access without firewall authentication to AS’s network. Firstly, lack of protection between its commercial business division and the rest leads to the exposure of the uncertainties of the internet. Lack of firewall in this case is leaving the clients confidential information, statistics, budgets, deadlines, contracts, employee information, strategies, deals open and exposed. This is an open exposure due to the uncertainties of the internet.

Any automated attacks or personal attack or attack to exploit the company secrets/statistics/data is the biggest threat to occur without the firewall. If this threat becomes real, the company’s data is lost or hijacked, client orders are stolen, budget scheduling and their deposit sections are exposed, fund transfers get out of hands and creates devastation in the company and its clients. Its formulas, designs and methodologies are exposed and might be sold to the rivals, thereby the company losing its competitive edge. This might even lead to the closure of the company.

To avoid this, firewalls should be established in such a way that, they support network address translation. Through this the internal internet uses private IP addresses to share information with public and the public can find the IP addresses static which avoids the tampering of data. Secondly, “ An invisible security weakness is lurking in most corporate networks in the form of millions of lines of code that represent the configuration scripts for all the devices on the network. ”.

In the network security diagram I find the main problem is that the firewall is established between the AS main router to router DD. This makes DD Santa Ana access AS network directly without the firewall. The firewall is misconfigured and is a major security threat. These misconfigured firewalls can possibly leave the network ports of the company open. If the hackers or attackers find the en ports, they can access the system of AS without any authorization. If this happens all the operations of AS should be held and comes to standstill.

The significance of the threat happening is high and consequences associated with it are severe. There is a possibility that their system might crash if this happens. If the system crashes, it will take long time to recover the information and takes a lot of budget required to set things right. This creates a financial drift in the company making the company lose its reputation in public. Software Vulnerabilities The main problems in software grounds are;

1. No proper records on the equipment installed and components purchased. 2. Installation of unsecured software on the system. 3. No replication of data. 4. Adoption of third party software vendors. The records of the AS show us the equipment installed, components purchased and software being used presently which has a marginal difference when compared on the onsite work plant. There are no records on the add on applications purchased to run the systems in AS. This leads to improper functioning of the systems in AS. This also leads to a threat where the employees can use this system for personal use making the system exposed to the outer world.

If this happens, there might be an outside chance for the company’s rivals know about their applications and software being used which reduces the company’s competitive edge. The unsecured software programs being installed on the employees system increases the possibility of malicious threats on the system. This might lead in the break through into the main server. If the main server is being tampered, it leads to breakage in the clients’ server. The clients cannot access AS network and causes the work to a standstill. The possibility of this occurring is low but the consequences of it are severe.

Another problem with the present AS software configuration is that they do not have their data replicated. They do have a backup but having their data replicated at the onsite plant is more important. If they lose their data, to decrypt their data from the backup might take them days or even weeks. This makes them to hold on to their advancements till they get the data back and thereby making the work standstill at the clients place. To avoid this, AS must be using PLEX, an invisible hard drive in the main server which holds the database of the company.

Recovering data from this is done in minutes and the main advantage of this is that no one can authorize the plex except the administrator. Finally, adoption of a third party software vendor delays the time in authorizing your software solutions. The emergency tasks cannot be finished on time if the vendor delays the software registration and verification. This threat is low in occurrence and the consequences of it are with medium severity. To avoid

such kind of threats, it’s better that AS develop their own software programs to hold the data together of have a direct contact deal with the vendors.