Computer

Business

This identified security problems from the computer systems to lack of security and potential threats. The second part looked at policy considerations and gave recommendations. This section dealt with systems personnel to information structure and ended with system certification recommendations. The third section detailed technical recommendation while the last section detailed management and administrative controls. With the increased and wide spread use of computers in the military, a need for procedures we due.

These procedure recommendations revolved around technique and security which ad not previously existed on such a broad scale.

Even with the large scale of operations, there still needed to be some privacy around the system and data that was shared or accessed. Through this study, batch, multiprogramming, and time- shared processing were all recommended for different levels of access and control. Three types of threats to system security were identified. These are accidental access of data, deliberate access of data, and a physical attack on the system. There were recommended safeguards to protect from all three vulnerabilities.

This protection ad to be Identified and secured by the system designer so not gaps were missed.

These gaps could be In the software, hardware, communication of Information and general lack of organization or the organization itself. There were recommended characteristic needs of the system seemed almost too massive to have all at one time. The system had to be flexible in term of performance, responsive to different conditions, dubitable for security

breaches, reliable, manageable, adaptable based on sensitivity needs, dependable, while assuring configuration integrity. With all of these emends, a definition list was put together so everyone could be clear on the document and the interpretation was consistent from person to person.

The second part of the study started out with fundamental principles and system personnel.

This detailed who could have access to what part of the system and the data. It also identified gate-keepers and administrators with user authentication guidelines. The data was organized and controlled so that any variance was identifiable. All transactions Into the system and the activity that took place was logged for transaction accounting. Auto-testing was Implemented and sufficient redundancy checks were put in place to ensure data control was not compromised.

Input and output parameters were very specific and access was obtained only through several checkpoints in the system.

The system was checked, tested, and evaluated often for any fail-points or weaknesses. Inspections were performed by experts to determine if the system was in compliance with predetermined requirements and regulations. System; design certification, installation certification, and recertification. The last part of the report detailed the technical recommendations. Due to the size of the system needed for the data-sharing, the present technology was insufficient and additional safeguards had to be put into place.

The central processing hardware had to have user isolation along with protection against unexpected access or conditions.

This meant that each user was unique and the program would isolate the data needed for that user. The software had to run with complex programs that allowed sorting and file copying while maintaining security checkpoints. This lead to access controls in different levels of the system. Certain users could only gain access to some information. If an unauthorized user tried to gain access to information outside their authority, a denial of access was sent.

This also generated a flag to be immediately checked.

All these steps and processes were new and now seem to be a very standard practice in the world of computers. Even with the most secure systems, there are still people or even other computer systems trying to gain access to data that they are not authorized to see or control. The cyber world continues to fill up with public and private data at tremendous speeds which will continue to lead the Uris's hacker to challenge themselves to getting data they should not have. 2. Consider the information stored on your personal computer.

For each of the terms listed, find an example and document it: threat, threat agent, vulnerability, exposure, risk, attack, and exploit.

Threats – this could be a person driving around your neighborhood looking for the insecure network. Threat Agent – this could be a hacker that finds the unsecured network with the intentions of installing a worm, computer virus,

or some sort of damaging program. Vulnerability – This could be an account that has a weak password like “ 123456”. Exposure – An example of this is when someone opens and e-mail with a Trojan, worm, or virus attached.

Risk – This could be an event in which you let someone you don’t know very well use your laptop or access a program without good intent. Attack – This is what happens when your system has been intentionally or unintentionally exposed to a malicious program or person.

Exploit – Can be gained at a local level or network level to take advantage of weaknesses or vulnerability in a system. They are used to gain control to a computer system. 3. Using the web, find out who Kevin Nitpick was. What did he do? Who caught him? Write a short summary of his activities and why he is famous.

Kevin Nitpick is know that he world’s most famous hacker according to his website (www. Interactivity. Com). In the early sass’s, he proved to be a computer genius that thrived on the breaking into high-profile company computers through the now out-of-date dial-up modem superhighway. He would assume false identities and cover his tracks to out run the FBI and other authorities looking to track him down.

He was finally caught and arrested in 1995 by the FBI in his North Carolina apartment, resourced four years later for wire fraud, computer fraud and identity theft.

Kevin Nitpick started his computer hacking at a seemingly young age of 1 5 gaining access to the Los Angels bus system. This lead to him obtaining free

rides on the public transport system. His first arrest for hacking came in 1988 when he was convicted of unauthorized access of a computer network in 1979 at the age of 16. This earned him a year in prison.

After his release, he continued his hacking using The Condor and became one of the Bi’s most wanted. After his arrest in 1995, it took four years to get conviction.

He had a lot of supporter that felt his conviction and incarceration was too harsh which include eight months in solidarity confinement since he was a perceived threat to national security.