Contents

Engineering, Computer Security

Contents Introduction 1 Task 1 1 Task 2 1 Task 3 1 3. 1 1 Data and Storage 1 3. 2 5 Authentication Process Plan 5 Considered Authentication plans 5 Reflective commentary 7 References 8 Introduction The report is being generated for the town council. The council has its main center and even operates sub smaller five neighborhood centers in various parts of town. The council solely relies on its network and data storage systems to interact with staff members and offices so that real time based data can be accessed regarding cases, clients etc. The data send over the network are very sensitive and vital for legal proceedings. Therefore the present system in the council needs to be enhanced. Different ways to implement security levels are to be discussed to implement or suggest the council the appropriate method. Task 1 Essential researches have been done about how to secure file storage and transfer considering the requirements. Further more details will be provided in Task 3. 1. Task 2 Different authentication methods and data security methods and on-going network monitoring plans have been analyzed which will be further discussed in Task 3. 2. Task 3 3. 1 Data and Storage A. Data Protection Issues As the town council deals with the legal services, the data transition should be secured very strongly. As the database of the council is larger and contains very vital information with it, different data protection issues are to be discussed. * The data stored in the hard drive may get corrupted leading to a huge data loss. * The database server may get crashed or get hacked. * As the data is being transferred to different many locations across the country, there is a high chance of eavesdropping. * Data sent through the network may get loss in the transition by an unauthorized access. * The data can be unwantedly modified

while on the process of transmission from the source to the destination network by hackers and eavesdropper. * The data can be infected on the process causing the destination network a massive loss by virus infection over the network. B. Data Protection Plans For Storage and Transmission For securing the data during the transmission several protection plans should be taken into considerations and should be followed through it. Following protection plans follows the DATA PROTECTION ACT 1998. * Personal data should be managed legitimately and properly. * Personal data should only be accessible for one person for more specified and lawful purposes. * Data should be adequate and relevant and should not excess the relation to the purpose they were created. * Data should be accurate and updated. * Data warehousing should be done for the additional security in the database. * Certain level of accessibility should be provided to the employees. * Firewalls policy should be implemented in order to ban social networking sites or any other sites that are not in the company policy. * Password authentication should be applied in order to provide the proper level of authentication to the employees. * Antivirus should be installed to prevent any kind of malicious program attack. * The transmitted data should be protected by different encryption method. Ciphering the data would help in the data. * Disaster plan should be made. Therefore, the backup of the whole data should be done in another safe location and should be updated with each operation concurrently. * VPNs should be created for securing the data in the public network. * Data logs should be created for the event that is taking place over the network and it should be monitored by the administrator frequently to keep track of the situation. Data Protection Plans (Shredders) C.

Alternative shielding approach For more feasible and effective way to protect the data, the organization can use different alternative methods. I. Data Masking It is the process of using different techniques to obscure or camouflage the specific data within a database table. A flat file certifying the data security is sustained and the crucial information is not leaked out of the authorized network. The masking algorithms are applied to the different multiple tables, applications and environments. Thus, the information integrity is maintained. Data Masking avoids the leaking of sensitive data to an unauthorized environment. [Data Masking: Grid Tools] Fig 1. 1: Data Masking II. Leased Line Leased line is a dedicated stable permanent connection between two networks in different locations. It is a private which only transports communications and traffic from one place to another in guaranteed level of service. The line can be used for data, VOIP and videos. It is most effective when sharing applications between two parties. It provides dedicated bandwidth and the data over the network is highly secured. Fig 1. 2: Lease Line 3. 2 Authentication Process Plan Various types of authentication process can be used for authenticating a user in the network. We need to come up with the most cost beneficial and efficient way. Practically feasible way for the town council could be: * Password and Pin code Authentication. In which the user needs to identify themselves with proper username and a password to gain access of data. * For security levels each department should be provided with a certain level of access in the resources. * Encryption process should be taken into the data. Exchange of public key and digital signatures should be done in the data for secure transition of the data. * IPsec should be implanted as it provides security

service at the IP layer. It maintains confidentiality and integrity of the data as well as authenticates the client in the network. Considered Authentication plans There are other way of authenticating the data in the network which were taken into consideration but then discarded as it provided less security on the data. * Password Authentication is of the simplest way to authenticate a user in the network. But it is easy for the hacker to crack the password by analyzing the flow of data in the network. * Biometric authentication was also taken into consideration. Though it is a secure method but it is an expensive way so it is not economically feasible. * SSL sessions was taken into consideration for the authentication process but as it provided less security than the IPsec, it was discarded. * Public key cryptography provides more security than the symmetric cryptography. As symmetric cryptography takes one key to crack, public key cryptography takes two key to crack the data. Ensuring the privacy security of data There are different way of method ensuring the data in the network. Some of the way are as follows: * Encrypting the data in MD5 algorithms or in RSA or Triple DES form using different encryption tools. * Different secure VPN protocols should be implemented in the network. PPTP and L2TP protocol can be used for securing the data transmission. * Firewall should be installed in order to protect the data and for filtering the network. * Intrusion detection system should be installed to detect malicious code in and over the network, * Policies should be implemented in the system dividing the department to a limit of access in the data. Considered Security Methods * There are several way of encrypting the data. But we choose the proposed encrypting than others as it is strong and conveniently fast to decrypt. * VPN networks are

reliable and secure way than any other protocols. As VPN provides more security options and features other options are considered. * Firewall policies are enough to secure the data and filter the network so that is why other antivirus programs with firewall features were taken into consideration. * Other security devices are neglected as intrusion detection system can provide enough security to the network. Vulnerabilities and Breach of System As it a huge network system in the system should be monitored very properly. Causes of the vulnerabilities in the system could be: * Software- Flaws in the new software. Many loopholes can be detected in the software and can be breached easily. * Organizations procedures-Poor password policy, lack of audits update. * Personnel- If the personnel are not well trained then the programs that are used by them may not be secure as they are not aware of any authentication or securing the method. These vulnerabilities in the system can be removed by monitoring the network. All the logs should be kept and updated by the administrator. Port scanners should be used by the network administrator to the test the network so as to look for vulnerability by attackers. Penetration Testing should be done in so as to find the loopholes in the network. Finding the possible threats from the network, administrator can provide the data to fix the vulnerabilities and upgrade the network security if possible. Reflective commentary According to the research the network should be implemented with the proposed security methods concurrently considering all the feasibilities of the organization. The proposed plan will provide authentication, confidentiality and maintains the integrity of the data. It will provide more secure data transmission in the network. It will provide more security within and outside

the offices. If the proposed plan are not feasible then alternative solutions are also provided so as to meet the requirements of the council. Through this assignment I have learned to consider different alternatives solution of securing the data in the network according to the needs and economic feasibility of the organization. References A summary of the Data Protection Act 1998[Online] http://www. abt-shredders. co. uk/popups/data_protection. htm[Accessed: 1st October 2012] Data Masking and Data Obfuscation for Sensitive Data Records [Online] http://www. grid-tools. com/solutions/data_masking. php [Accessed: 1st October 2012] Lease Line, Leased Lines, What is Lease Lines? Benefits? [Online] http://www. datanet. co. uk/leased_lines. aspx[Accessed: 1st October 2012]