Executive proposal project research proposal samples

Law, Security

The security of both the servers and Workstations which run on Windows environment has been a key challenge for institutions, companies and even private entities. Different technological companies have tried to come up with security protection software which will guarantee maximum protections to both servers and the workstations. It is the wish of each and every chief information security officer to have 24x7 security support at the time. Kaspersky endpoint security for Windows is the most appropriate security solution both servers and workstations which run on Windows environment. This security software was developed to meet the business technological changes for small, medium size and large business organization. The software also gathers for institutional changes in terms of content filtering. The developer put consideration on the fact that there are tremendous technological changes, and as such there is the need for state of the art security software that responds to the pressures exerted by the cloud based technologies.

It is indisputable that the technological trends pose critical and fatal malware risk to the organizations. Kaspersky panda enables the user to embrace the state of the art technologies and feel satisfied as far as security and protection are concerned. Being the cornerstone of Kaspersky security protections, Kaspersky endpoint security 8 gives a centralized security for servers and workstations which run on Windows against network attacks and dangerous programs.

The first cyber attack that Kaspersky Endpoint Security for Windows will handle is key logging and spyware. This is a malware that is built to illegally track and block the right of the user to get access to the system. An example

of this attack is where someone or an individual tries to log on to the system or website like an email account, but the system or the site fails to authenticate the user. To prevent these, system administrators should establish a mechanism where if the user complaints of such issue the system should prompt the user by asking some questions relating to the account.

The second attack is backdoor or command/control. These are weapons that give remote access that are created to divert the functionality of the system. It is one of the dangerous SQL injection attacks. This is a unique attack that targets the web pages of the system application. It cuts down the communication between the database and the system application interface. This attack is common in the organization where system implementation is taking place. An example is a situation where an attacker alters the name of the database and hence disconnects it from the user interface.

The software also handles packet sniffing. This is the attack data on transit. The attacker tracks and collects the data in the network for malicious use. He can modify this data and send wrong data to the recipient or can divert the data causing denial of service. Situation whereby the policy information or business transaction information of a company that is suppose to reach the stakeholders are redirected and send to the competing firm is a very good illustration.

The software also Proxy authorship features. Once individual identity details are recorded and well documented, he/she will fear to engage in any fraudulent activity because tracking can be done in case of any fraud. Any employee that uses the system must log on using the user name and password that expires every two weeks and should be renewed by making a

request so that the administrator is aware. To stop this attack, the system developers should limit the number of attempt that one can enter a password before the system completely block (Rosenberg 2006). This can be enabled by using the GPO in the active directory where the system block by either redirecting the user interface of the system or completely hide. It can also make the form inactive or ask for verification using related questions Kaspersky Endpoint Security for Windows is a multilevel security solution. The four security feature that is targeted by Kaspersky Endpoint Security for Windows is confidentiality, integrity, authenticity and availability. Confidentiality is the process whereby the security team strives at ensuring that there is limited or totally no unauthorized person gains access of the information in the system. Integrity aims at maintaining the correctness and accuracy of the information that is used to carry out certain operation. Availability is to ensure that information or data is available any time the user needs. Authenticity is all about the ability of a computer to recognize the right user when he or she enters the authentication credentials (Salomon 2007).

Kaspersky Endpoint Security for Windows also provides securities ageist operating system attack. At the operating system level, the security mechanism targets the issues that are brought about unauthorized processes and users. The key advantage of this security mode is its aim to ensure that the individual that gain access to the network, memory and files have the authority to access. Operating system is one of the sections that require controlled. Components that are provided by operating system running in a particular computer are used to provide security in middleware

level. The enforcement of this mechanism is by use of a monitor that becomes the reference and mediator of any trial that is made as far as accessing the computer resources is concerned. This monitor queries the database that contains identification information for all users and processes that has permission to use them in order to decide whether one is allowed or not authorized. Any operation that the user tries is also tested to check if it is allowed before it is performed. The authorization timelines are set by the person that has the right to manage, for example, the security administrator. The security policy that the organization has put in place is the basis of setting the authorization. With the permission from the administrator, the user can change some settings for example, installing a new program that will run in the machine. This is the responsibility of the operating system (Middleton 2005).

There two of protection that access control can provide to the system at the operating system level. Requirements that an operating system need to put into consideration involve necessity to take care of every individual's resource and at the same time enable sharing of resources in a balanced manner. It provides memory protection and Information flow control

The major advantage of memory protection is that it is essential in an environment where multiprogramming takes place. Protection is needed to ensure that all the processes that are running within a given period are working correctly. This is done by separating the space of memory that holds different processes by use of a scheme called virtual memory. This is a memory management scheme that uses paging, segmentation or both as tools to manage the memory.

There two measures that are used provide the accessibility control of system that process data. These are: Access control that is user oriented which is also called authentication. In most system that are shared among different users or those computers which access the data stored by a server. A system that requires the credentials of the user is put in place. The system will request the user to enter the identification or username and also a password. Log system can be stand advantages running in each single computer or the administrator can configure in a single administrator computer that is used to control all the other workstations in a centralized point. The rest of the workstation computers will access this service via a network to determine the authenticity of an individual that tries to log in to the computer. For computers that run stand advantages system. The network is taken to represent transport communication link that the user is permitted to make use of it (Wall 2009).

Another access control is data-oriented that takes place after the user has been allowed to make use of application and the host and therefore he or she needs to access data. Basing on the above, the operating system protection models applied real time is required. These are mandatory access control and discretionary access control. In the previous that is also termed as multilevel access control, data or information are grouped according to the different sensitivity that are required to be administered. The security clearance is given to every user. Determination of access right is based on the correlation between the clearance of the user and the sensitivity level that a certain class of information is accorded. The two models that are designed to use this access control model are Bell-LaPadula and Lattice

models.

For discretionary access control, the information that is stored in the computer has owners that are unique. Each owner has the total right to use the information alone and should remain discrete according to the matrix model that is used for DAC allocation of objects (Yar 2006).

This is a security approach that permits the person that wrote an application to have the control of how the data flow between different applications that runs in the computer and also the exchange with the outside environment. The basis of this security model is to permit software that are not trustworthy to carry out computing procedures with data that is private while the release of these data is managed by code that are trusted. The essence of this is to protect malware that can be contained in the not trusted program.

These particular security approach advantages include its ability to control the flow of even the finest information and at the same time offer performance that is very high. In addition, the DIFC flume model an extension that enables programmers to implement the security control since the language that is used is more common to programmers

The major disadvantage that this security model faces is the fact that the performance of the operating system is compromised. In addition, there are some bugs that can be contained in both trusted and non trusted program that can bring risk by violating the security policy that is put in place. More so, there some security vulnerability on the operating system that runs since the base that is used for flume trusted computing environment is

comparatively larger. In addition, the performance of the operating system is affected negatively and hence can lead to integration of the kernel.

References

Middleton, B. (2005). Cybercrime investigator's field guide. Auerbach Publications.

Ransome, J., & Rittinghouse, J. (2009). VoIP security. Digital Press.

Rosenberg, R. S. (2006). The social impact of computers. Emerald Group Publishing.

Salomon, D. (2007). Data privacy and security. Springer.

Trevor, J. (2011). Cyber Attack: Improving Prevention and Prosecution" Hearing Before the Subcommittee on Technology, Terrorism. General Books.

Wall, D. (2009). Crime and the Internet. Routledge.

Wiles, J., & Cardwell, K. (2007). The best damn cybercrime and digital forensics book period. Syngress.

Yar, M. (2006). Cybercrime and society. SAGE.