Trusted computing base business reasons for a bcp and a drp

Technology, Information Technology

nExtract of sample " Trusted computing base / Business reasons for a BCP and a DRP" n

nNumber: Lecturer The concept of a “ trusted computing base” Trusted computing base was first defined by as the combination of kernel and trusted process that allow violation of the systems access and control regulations (Rushby, 1981). Lampson further defined it as a small amount of software and hardware that security depends on and that we distinguish from a much larger amount that can misbehave without affecting security (B. Lampson, 1992). From these two definitions therefore, trusted computing base can be terminology in computer security meaning a set of all the components including hardware, software, procedures and all other relevant components that are critical and essential to enforcing the security of the entire system. In essence any vulnerability that may be faced by the trusted computing base will jeopardize the security of the entire system. This aspect places the TCB as a major and critical element of any system (Merkow & Breithaupt, 2006). For this reason the TCB should be carefully designed and implemented in order to realize a reliable system security. To achieve this modern operating system have immensely reduced the size of the TCB to a reasonable capacity that can easily be exhaustively examined and audited more effectively and efficiently (Merkow & Breithaupt, 2006). The boundaries and scope of a TCB is defined at the organizational level by a security policy that is used in the organization. The development of a security policy should therefore be done exceptionally well so as to incorporate a well structured TCB. It is therefore evident that the TCB boundary is determined by the target of evaluation (TOE) in the security process. The target evaluation in any normal scrutiny of the system and the subcomponents, the list of components and the boundary under scrutiny should be determined before hand (Rushby, 1981). According to the orange book this concept is further explained that the ability of a trusted computing base to enforce correctly a unified security policy entirely depends on the accuracy of the mechanisms within the trusted computing base, the protection of those mechanisms to ensure their correctness and the correct input of parameters related to the security policy (B. Lampson, 1992). This basically means specific resources such as hardware and software are part of the TCB if it has specifically been designed to provide the security to the computer system. In the modern computer systems TCB is responsible for authenticating and controlling access by the users and their programs to files/file systems, memory and peripherals. Additionally the TCB is also responsible for the integrity checking of the communication path between the user and the computer. A report by James p. Anderson lays out some principles that a TCB must subscribe to (Rushby, 1981): 1. The process of decision making and the arrival at the decisions must not be tampered with. 2. It is fundamental that the TCB is always involved in security decision making. 3. The TCB must be of small size to allow exhaustive analysis and testing to assure its accuracy and correctness. References B. Lampson, M. A. (1992). Authentication in Distributed Systems: Theory and Practice. ACM Transactions on Computer Systems . Merkow, M., & Breithaupt, J. (2006). Information Security: Principles and Practices. New Jersey: Pearson Education. Rushby, J. (1981). " Design and Verification of Secure Systems". 8th ACM Symposium on Operating System Principles. Pacific Grove, California, US. 2. What are the different business reasons for a BCP and a DRP? Business continuity plan and disaster recovery plan are two terms that are mostly used interchangeably. However there is a slight difference between the two terms as used in business systems (4service Inc, 2012). Data Recovery Planning is concerned with the recovery of systems and infrastructure components incase of any failure in the system on the other hand Business Continuity Planning is concerned with a wider scope that involves the determination of which system components and functions need to be restored and those that may be ignored (IBM, 2011). In the current technological age all organization are employing technology and information systems to carry out their day to day activities. This information systems and technology are vulnerable to threats and as a result lead to loss of data and information, unauthorized access and manipulation of data and information and the eventual alteration of the activities in the organization. For this reasons the use of BCP and DRP are inevitable to minimize losses, unauthorized access and also minimize impacts as a result of these threat (Merkow & Breithaupt, 2006). From a business perspective, the ultimate goal and importance of having a BCP and a DRP is basically to ensure there is business continuity even when there is technical or system failure in the business. This minimization of interruption to business operation reduces the loss in monetary terms and time in the business. It also minimizes disruption to suppliers and customers thus enhancing acceptability, credibility and integrity of the business. According to the British standard BS 31100 BCP identifies the potential threats to the organization and the impacts that this threats may have on the business in the event of their occurrence. The BCP thus builds organizational resilience and preparedness for any eventuality and ensures continuity of business. This safeguards and protect s the interests of their stakeholders. The DRP aides in the event of an occurrence of a disaster, this provides laid down procedures and documented and tested recovery plan (IBM, 2011).

References 4service Inc. (2012). importance of business continuity planning. Retrieved March 20, 2013, from 4service: http://www. 4service. com/importance_of_business_continuity_planning. asp IBM. (2011, August 1). disaster Recovery and business continuity. Retrieved March 21, 2013, from IBM: http://www-304. ibm. com/partnerworld/gsd/solutiondetails. do? solution= 44832&expand= true&lc= en Merkow, M., & Breithaupt, J. (2006). Information Security: Principles and Practices. New Jersey: Pearson Education.