DOWNLOAD PDF FUNDAMENTALS OF INFORMATION SYSTEMS SECURITY 2ND

Chapter 1 : Fundamentals of Information Systems Security

Revised and updated with the latest information from this fast-paced field, Fundamentals of Information System Security, Second Edition provides a comprehensive overview of the essential concepts readers must know as they pursue careers in information systems security.

Job Rotation[edit] Job Rotation is an approach to management development where an individual is moved through a schedule of assignments designed to give him or her a breath of exposure to the entire operation. Job rotation is also practiced to allow qualified employees to gain more insights into the processes of a company and to increase job satisfaction through job variation. Separation of Duties[edit] Separation of duties SoD is the concept of having more than one person required to complete a task. It is alternatively called segregation of duties or, in the political realm, separation of powers. Without those few and far between expert level techs who can have or get the administration rights to view all aspects of any given production process it will be nearly impossible to determine the underlying cause and can lead to outrageous decisions as to what the problem must of been. Or nobody realizing the automated software machine was running into RAM issues because every automated job was set to auto start at exactly 6: With the concept of SoD, business critical duties can be categorized into four types of functions, authorization, custody, record keeping and reconciliation. In a perfect system, no one person should handle more than one type of function. In information systems, segregation of duties helps reduce the potential damage from the actions of one person. IS or end-user department should be organized in a way to achieve adequate separation of duties Control Mechanisms to enforce SoD There are several control mechanisms that can help to enforce the segregation of duties: Audit trails enable IT managers or Auditors to recreate the actual transaction flow from the point of origination to its existence on an updated file. Good audit trails should be enabled to provide information on who initiated the transaction, the time of day and date of entry, the type of entry, what fields of information it contained, and what files it updated. Reconciliation of applications and an independent verification process is ultimately the responsibility of users, which can be used to increase the level of confidence that an application ran successfully. Exception reports are handled at supervisory level, backed up by evidence noting that exceptions are handled properly and in timely fashion. A signature of the person who prepares the report is normally required. Manual or automated system or application transaction logs should be maintained, which record all processed system commands or application transactions. Supervisory review should be performed through observation and inquiry and the trust built with directory one-level up managers. To compensate repeated mistakes or intentional failures by following a prescribed procedure, independent reviews are recommended. Such reviews can help detect errors and irregularities but are usually expensive can raise questions as to how much can an outside independent review once a quarter know about your processes compared to people within and what level of trust can be built with those independent reviewers. Least Privilege Need to Know [edit] Introduction The principle of least privilege, also known as the principle of minimal privilege or just least privilege, requires that in a particular abstraction layer of a computing environment every module such as a process, a user or a program on the basis of the layer we are considering must be able to access only such information and resources that are necessary to its legitimate purpose. This principle is a useful security tool, but it has never been successful at enforcing high assurance security on a system. Benefits Better system stability. When code is limited in the scope of changes it can make to a system, it is easier to test its possible actions and interactions with other applications. In practice for example, applications running with restricted rights will not have access to perform operations that could crash a machine, or adversely affect other applications running on the same system. When code is limited in the system-wide actions it may perform, vulnerabilities in one application cannot be used to exploit the rest of the machine. In general, the fewer privileges an application requires the easier it is to deploy within a larger environment. This usually results from the first two benefits, applications that install device drivers or require elevated security privileges typically have addition steps involved in their deployment, for example on Windows a solution with no device drivers can be run directly with no installation, while device drivers must be installed separately using the Windows installer service in order to grant the driver elevated privileges Mandatory Vacations[edit] Mandatory vacations of one to two weeks are used to audit and verify the work tasks and privileges of employees. This often results in easy detection of abuse, fraud, or negligence. Job Position Sensitivity[edit] Security Roles and Responsibilities[edit] Levels of Responsibilities[edit] Senior management and other levels of management understand the vision of the company, the business goals, and the objectives. Functional management, whose members understand how their individual departments work, what roles individuals play within the company, and how security affects their department directly. Operational managers and staff. These layers are closer to the actual operations of the company. They know detailed information about the technical and procedural requirements, the systems, and how the systems are used. The employees at these layers understand how security mechanisms integrate into systems, how to configure them, and how they affect daily productivity. Classification of Roles and their Responsibilities[edit] Data Owner The data owner information owner is usually a member of management, in charge of a specific business unit, and is ultimately responsible for the protection and use of a specific subset of information. The data owner decides upon the classification of the data that he is responsible for and alters that classification if the business needs arise. This person is also responsible for ensuring that the necessary security controls are in place, ensuring that proper access rights are being used, defining security requirements per classification and backup requirements, approving any disclosure activities, and defining user access criteria. The data owner approves access requests or may choose to delegate this function to business unit managers. And it is the data owner who will deal with security violations pertaining to the data he is responsible for protecting. The data owner, who obviously has enough on his plate, delegates responsibility of the day-to-day maintenance of the data protection mechanisms to the data custodian. Data Custodian The data custodian information custodian is responsible for maintaining and protecting the data. System Owner The system owner is responsible for one or more systems, each of which may hold and process data owned by different data owners. A system owner is responsible for integrating security considerations into application and system purchasing decisions and development projects. The system owner is responsible for ensuring that adequate security is being provided by the necessary controls, password management, remote access controls, operating system configurations, and so on. This role needs to ensure that the systems are properly assessed for vulnerabilities and must report any to the incident response team and data owner. The security administrator role needs to make sure that access rights that are given to users support the policies and data owner directives. Security Analyst This role works at a higher, more strategic level than the previously described roles and helps to develop policies, standards, and guidelines and set various baselines. Whereas the previous roles are "in the weeds" and focusing on their pieces and parts of the security program, a security analyst helps define the security program elements and follows through to ensure that the elements are being carried out and practiced properly. This person works more at a design level than at an implementation level. Application Owner An application owner, usually the business unit managers, are responsible for dictating who can and cannot access their applications, like the accounting software, software for testing and development etc. Change Control Analyst The change control analyst is responsible for approving or rejecting requests to make changes to the network, systems, or software. This role needs to make sure that the change will not introduce any vulnerability, that it has been properly tested, and that it is properly rolled out. The change control analyst needs to understand how various changes can affect security, interoperability, performance, and productivity. Data Analyst The data analyst is responsible for ensuring that data is stored in a way that makes the most sense to the company and the individuals who need to access and work with it. The data analyst role may be responsible for architecting a new system that will hold company information or advising in the purchase of a product that will do this. Process Owner Security should be considered and treated like just another business process. The process owner is responsible for properly defining, improving upon, and monitoring these processes. A process owner is not necessarily tied to one business unit or application. Complex processes involve a lot of variables that can span across different departments, technologies, and data types. Solution Provider This role is called upon when a business has a problem or requires that a process be improved upon. User The user is any individual who routinely uses the data for work-related tasks. Product Line Manager Responsible for explaining business requirements to vendors and wading through their rhetoric to see if the product is right for the company Responsible for ensuring compliance to license agreements Responsible for translating business requirements into objectives and specifications for the developer of a product or solution Decides if his company really needs to upgrade their current systems This role must understand business drivers, business processes, and the technology that is required to support them. The product line manager evaluates different products in the market, works with vendors, understands different options a company can take, and advises management and business units on the proper solutions that are needed to meet their goals.

Chapter 2 : Information Security Fundamentals, 2nd Edition - PDF Free Download - Fox eBook

Revised and updated with the latest data in the field, Fundamentals of Information Systems Security, Third Edition provides a comprehensive overview of the essential concepts readers must know as they pursue careers in information systems security.

Chapter 3 : ISBN - Fundamentals of Information Systems Security 2nd Edition Direct Textbook

PART OF THE JONES & BARTLETT LEARNING INFORMATION SYSTEMS SECURITY & ASSURANCE SERIES Revised and updated with the latest information from this fast-paced field, Fundamentals of Information System Security, Second Edition provides a comprehensive overview of the essential concepts readers must know as they pursue careers in information systems security.

Chapter 4 : Fundamentals of Information Systems Security - Wikibooks, open books for an open world

Start studying Fundamentals of Information Systems Security (2nd Ed) Chapter 6. Learn vocabulary, terms, and more with flashcards, games, and other study tools.

Chapter 5 : Applied Labs | Information Systems Security & Assurance Curriculum

PART OF THE JONES & BARTLETT LEARNING INFORMATION SYSTEMS SECURITY & ASSURANCE SERIESRevised And Updated With The Latest Information From This Fast-Paced Field, Fundamentals Of Information System Security, Second Edition Provides A Comprehensive Overview Of The Essential Concepts Readers Must Know As They Pursue Careers In Information Systems Security.

Chapter 6 : Fundamentals Of Information Systems Security 2nd Edition

PART OF THE JONES BARTLETT LEARNING INFORMATION SYSTEMS SECURITY ASSURANCE SERIES Revised And Updated With The Latest Information From This Fast-Paced Field, Fundamentals Of Information System Security, Second Edition Provides A Comprehensive Overview Of The Essential Concepts Readers Must Know As They Pursue Careers In Information Systems Security.

Chapter 7 : Fundamentals of Information Systems Security - David Kim, Michael G. Solomon - Google Boo

Information Processing and Security Systems is a collection of forty papers that were originally presented at an *international multi-conference on Advanced Computer Systems (ACS) and Computer Information Systems and Industrial Management Applications (CISIM) held in Elk, Poland.*

Chapter 8 : A. Answer Key - Fundamentals of Information Systems Security [Book]

Fundamentals of Information System Security provides a comprehensive overview of the essential concepts readers must know as they pursue careers in information systems security. The text opens with a discussion of the new risks, threats, and vulnerabilities associated with the transformation to a digital world, including a look at how business.

Chapter 9 : [PDF]Fundamentals of Information Systems Security - Free Ebooks download PDF- blog.quint

Information Security refers to the practices and methods which are designed and enforced to shield electronic, print, or any other kind of confidential, private and sensitive information from unauthorized access.