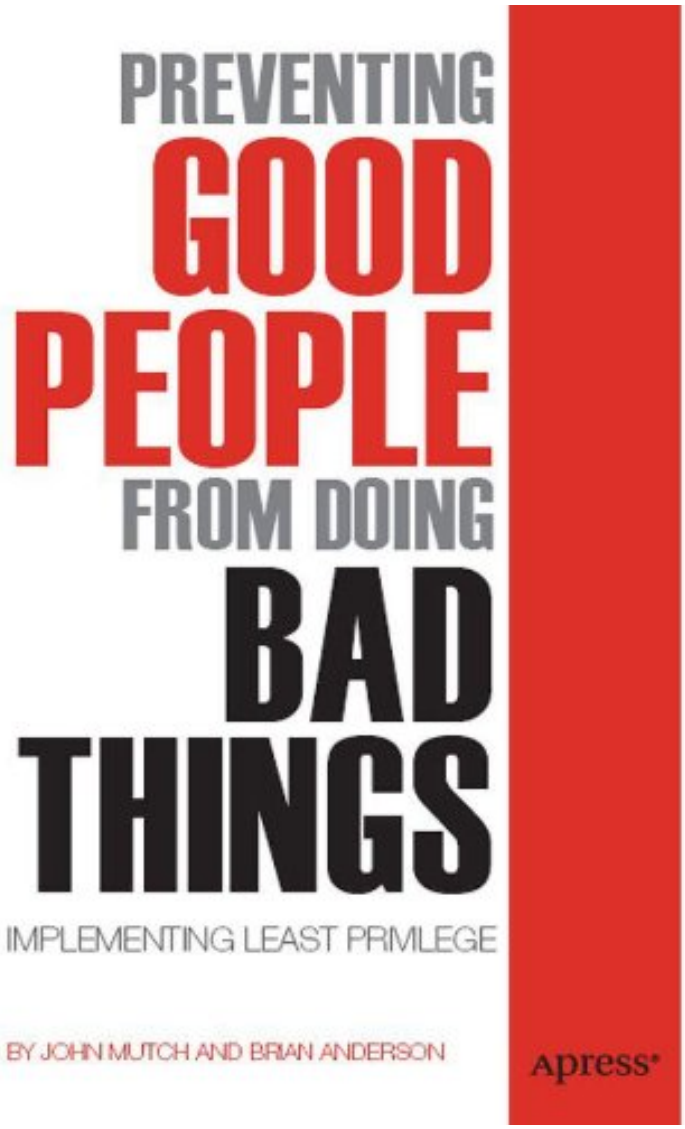
Preventing Good People From Doing Bad Things: Implementing Least Privilege

John Mutch, Brian Anderson
*ebooks | Download PDF | *ePub | DOC | audiobook*



#2322002 in eBooks 2011-10-17 2011-10-17File Name: B00642246Q | File size: 27.Mb

John Mutch, Brian Anderson : Preventing Good People From Doing Bad Things: Implementing Least Privilege before purchasing it in order to gage whether or not it would be worth my time, and all praised Preventing Good People From Doing Bad Things: Implementing Least Privilege:

4 of 4 people found the following review helpful. For those looking to get a handle on the topic, an excellent resourceBy Ben RothkeFor anyone who ever had to prepare for the CISSP exam, the principle of least privilege is often ingrained in their short-term memory. The bigger problem is that given the importance of least privilege, it is

often forgotten at the enterprise level, and frequently least implemented correctly.Specifically, least privilege is the notion that in a particular abstraction layer of a computing environment, every module (such as a process, a user or a program depending on the subject) must be able to access only the information and resources that are necessary for its legitimate purpose.Much has been written about the topic, but not about what to do to implement it. In Preventing Good People From Doing Bad Things: Implementing Least Privilege, the authors note that many companies have spent huge amounts of money on information security hardware and software, but don't make allowances to deal with what is often the weakest link in the organization, end-users.In 11 easy to read chapters containing fewer than 200 pages, the book provides a good high-level overview of the concepts of least privilege. The book does not get into the details of access control on various operating systems, as that would triple the books length. Rather it details what happens when user rights are not adequately limited, and gives stories of the effects of unlimited administrator level rights.While for the most operating system agnostic, the book does provide ways in which to living Active Directory rights in chapter 4, and touches similar concepts in Unix and Linux, as well as virtualization in chapter 6.The title of chapter 2 pretty much sums up the entire book and concept - Misuse of privilege is the new corporate landmine. The authors quote Mark Diodati of Gartner that "organization continues to struggle with excess user privileges as it remains the primary attack point for data breaches and unauthorized transactions".Another crucial topic us databases, discussed in chapter 8. Far too many DBA's have unfettered and unmonitored access across terabytes of data that can often lead to serious breaches.The book concludes with some good ideas on how to break bad habits within IT. These pragmatic suggestions include (obvious) suggestions such as: stop allowing employees access to rook, not letting desktop users run as administrator, that hat just because a firm is using access control, that they are immune to data breaches, and more.For those looking to get a handle on the topic, they will find Preventing Good People From Doing Bad Things: Implementing Least Privilege an excellent resource.

In today’s turbulent technological environment, it’s becoming increasingly crucial for companies to know about the principle of least privilege. These organizations often have the best security software money can buy, with equally developed policies with which to execute them, but they fail to take into account the weakest link in their implementation: human nature. Despite all other efforts, people can sway from what they should be doing. Preventing Good People from doing Bad Things drives that concept home to business executives, auditors, and IT professionals alike. Instead of going through the step-by-step process of implementation, the book points out the implications of allowing users to run with unlimited administrator rights, discusses the technology and supplementation of Microsoft’s Group Policy, and dives into the different environments least privilege affects, such as Unix and Linux servers, and databases.Readers will learn ways to protect virtual environments, how to secure multi-tenancy for the cloud, information about least privilege for applications, and how compliance enters the picture. The book also discusses the cost advantages of preventing good people from doing bad things. Each of the chapters emphasizes the need auditors, business executives, and IT professionals all have for least privilege, and discuss in detail the tensions and solutions it takes to implement this principle. Each chapter includes data from technology analysts including Forrester, Gartner, IDC, and Burton, along with analyst and industry expert quotations. What you’ll learnWhy unlimited administration rights are a bad thing Why least privileges is a good solution Effective implementation of least privileges Least privileges on Unix and Linux servers Issues with Microsoft's Group Policy Who this book is forThe audience is segmented into three separate categories, all of which are clearly addressed and weighed-in on in each chapter: the auditor, the businessman, and the IT professional. Auditor The first segment are the information technology security auditors. They are the ones responsible for the analysis of technical, physical, and administrative controls in the organization(s) whose security is in question. Their work includes the auditing of data center personnel, computer equipment, all policies and procedures, physical and environmental controls, and back-up procedures. Because their jobs so heavily rely on established protocols for the protection of sensitive information, this segment of the market will find this book a must-read. Their main concern is making sure the companies they are inspecting are in compliance with regulations and are taking the appropriate measures to secure their information and the users accessing them. They will learn how least privilege is the only way to fully satisfy government security regulations, and it will give them necessary and cutting-edge information on how to correctly perform their jobs. Businessperson The second segment are the businesspeople. They are the ones who run the companies requiring least privilege. These individuals are driven by the bottom line, and are ultimately concerned with spending and returns on investment. While they may be interested in security and realize its importance, the motivation behind any decisions is saving the company money. They need this book because it will clearly outline the financial benefits of implementing least privilege. It will explain that, from a business point of view, least privilege is the only way to eliminate the misuse of privilege and avoid the extensive costs of security breaches, expensive audits, help desk costs, and costly hours of IT troubleshooting. They will read it and use it as a reference as they prepare financially for a more secure IT environment. IT Professional The third and final segment are the IT professionals. They are the ones who appreciate security for security’s sake. They understand the implications of a noncompliant environment. They are on the forefront of the company’s information environment. They manage users and those users’ privileges. They download

applications, grant privileges t

About the AuthorBrian Anderson brings more than 25 years of global enterprise software and security industry experience to BeyondTrust, where he will be responsible for all aspects of corporate brand development, lead and demand generation to increase awareness and interest in all customer and investor segments. In addition, he will be responsible for building a VAR channel to expand distribution for BeyondTrust products globally. Prior to BeyondTrust, Anderson served as a serially successful chief marketing officer for several venture-funded companies. At Siderean Software, his branding efforts garnered rave reviews and numerous awards, including innovator status in the Gartner Magic Quadrant. At Avamar Technologies, his leadership resulted in a huge revenue increase and numerous awards. Avamar was subsequently acquired by EMC. Prior to Avamar, Anderson was director of marketing at IBM s Tivoli Security and Storage, a role he inherited after successful building industry leader Access360 s brand and sales pipeline through successful positioning for a sale to IBM. Anderson also served as chief marketing officer of HNC Software, which experienced tremendous growth during his tenure and was successfully acquired by Fair Isaac in 2002. Anderson served for seven years prior to HNC at FileNet Corporation, culminating in his role as vice president of worldwide corporate marketing. At FileNet, Anderson built a tremendous global channel organization that ultimately represented almost 50 percent of the company s revenue. He received his bachelor of science degree in computer science from the University of New Orleans.