Defend IT: Security by Example

Ajay Gupta and Scott Laliberte
Addison Wesley Professional, 2004
$34.99 (paper), 384 pp.
ISBN 0-321-19767-4

Reviewed by Gary Dobbins

For IT leaders addressing the challenge of securing their IT operations, and for the practitioners who will undertake the task, *Defend IT: Security by Example* provides an excellent introduction to a broad sample of the threats and responses that occupy the daily life of an IT security professional. From the opening question ("What does a cybersecurity professional do?") and throughout the case studies that compose the rest of the book, the authors' style enables readers to feel as though they are veteran security professionals trading war stories with colleagues.

Several aspects of an overall security program are covered, each in an enlightening, and sometimes entertaining, series of individual case studies rather than as a traditional (and sometimes dry) sequence of topics. The authors chose this approach due to positive feedback on their previous book's use of illustrative case studies. Each chapter effectively draws the reader into the topic through its story and continues to engage the reader by including ample details about the various problems and the solutions chosen for each.

Defend IT: Security by Example includes recommendations that should be part of every IT organization's security architecture and describes tools and skills that every IT security practitioner will want in their arsenal.

The 16 case studies follow:

- *Getting to know the enemy: Nmap the target network*

The authors wisely chose to lead with this story because it's always helpful to have an understanding of the motives and mindset of those who might be trying to overcome your security defenses. During the course of this study, some myths are dispelled and several useful defensive techniques revealed.

- *Home architecture*

Someone once said that if you don't know where you are, a map won't help, and if you don't know where you're going, any map will do. This chapter helps illustrate why a network architecture chosen to accommodate a balance of factors—performance as well as defensibility—can actually become one of your layers of defense, instead of merely being the highway that leads attackers to your door. Good advice is included regarding the temptation to build solely for convenience or performance, and how doing so can lead to a network design that is less secure in subtle yet risky ways.

- *No service for you!*

In a university environment, denial-of-service (DoS) attacks typically use networks as weapons directed elsewhere. At other times, university services may be the intended target. Unfortunately, our services tend to suffer regardless of the direction in which the attack is aimed. Loss of service availability through a DoS attack can be disastrous if we are less prepared to deal with this sort of attack than with events we have anticipated, such as hardware failures. An effective DoS attack for which we're unprepared can quickly take the situation outside our ability to control. Here, the authors relate the ways such attacks are mounted and what we can do to reduce their consequences.

- *Look, Ma, no wires!*

There is no shortage of wireless networks at institutions of higher learning, and likewise no shortage of options for securing them. Our institutions may be among the best prepared to address wireless security, due to the effective and timely work being done by inter-institutional teams of engineers working through EDUCAUSE. The authors provide several valuable insights into the myriad factors one must consider in any wireless security plan; show how would-be intruders can perform reconnaissance; and reference recommendations from the National Security Agency (NSA) and the Department of Defense (DoD).

- *Virus outbreak (two cases)*

The first case study illustrates how a "temporary" change, effected to enable collaborative access to a system, turned out to become the gateway that allowed an attack to succeed with alarming consequences. Good evidence is visible here for not one but a layered set of defenses, as well as support for effective patch management.

The second of these studies provides an example of a worm outbreak that became a pervasive problem for the victim. The study describes the response, which consisted of organizing an incident-response team, coordinating their activities, and preparing them for future incidents. An incident-response strategy emerges; after the strategy is mapped and procedures have been adjusted, the strategy forms the basis for response to future outbreaks.

- *Changing face*

Reputation is one of an institution's more important assets, which, in an increasingly online culture, could suffer if its Web presence were damaged. Gangs of attackers actually form clubs with contests to see who can deface the most sites in the shortest time. To help the reader avoid being one of their statistics, this chapter points out some easily followed practices.

- *Protecting borders: perimeter defense with an IDS*

Selecting a tool, such as an intrusion detection system (IDS) to assist the security team with detection of anomalous activity and virus infections, can be a daunting task. New vulnerabilities and attacks are continually appearing, and the feature sets of various products evolve as well. An IDS can help answer the question of whether a particular type of hostile activity is happening at one's institution. The authors provide a useful guide to selection criteria; very handy when venturing into the realm of these products.

- *Disaster all around*

Perhaps the most intriguing of all the chapters, here the story unfolds telling how an unanticipated form of disaster led to significant consequences. Despite what appear to be effective preparedness measures, the worst did still happen in this case. After many dollars spent and jobs lost, the response team's actions produced a positive and effective result using the lessons learned.

- *Security is the best policy*

In the authors' own words, policy "sets the tone for how seriously an organization takes its security." Without effective and applicable policy, security actions become merely tactics, or, worse, they may be doomed to fail. The authors provide a template—in a very approachable and usable form—for development of policies, followed by an illustration of their use in one organization.

- *HIPAA: security by regulation*

This chapter describes one company's approach to compliance with the regulatory stipulations regarding security practices surrounding relevant data. The text does not attempt to provide a cookbook for compliance. Rather, it shows the company in question responding proactively to the actions required of them, first through assessment, then reformation of internal practices.

- *A war-dialing attack*

No security text would be complete without an example of how a seemingly innocuous presence of a modem can undermine the effectiveness of an institution's overall (and otherwise effective) security program. The chapter concludes with a simple yet important policy recommendation.

- *A low-tech path into the high-tech world*

Social engineering—using human responses and tendencies as a means to overcome defenses—is an increasingly common vector for penetrating a site's defenses. Consider the recent round of "phishing" schemes, where a message is used to trick people into visiting a Web site or otherwise introducing a hostile program onto their system. Human-caused virus infections are increasingly taking the place of viruses' dependence on weak protections. This shift is perhaps due to the increased presence of effective antivirus defenses. If a door is properly locked, then the next easiest means to entry may be to simply trick the occupant into inviting you in.

- *Industrial espionage*

Although this chapter deals with a case that occurred in a corporate setting, the issues it illustrates regarding defense of intellectual property make it relevant to institutions of higher learning. Moreover, the chapter provides an excellent insight to the process of a forensic investigation and provides the reader with useful references to regulations and other requirements that should govern such an investigation.

- *Executive fraud*

In conjunction with the preceding chapter, here the forensics process is shown in a new light—investigation of alleged "insider" malfeasance. Easily misperceived as a threat that only others face, insider misdeeds here receive some deserved attention. Again, the authors raise key questions regarding the handling of evidence, chain of custody, and even presumption of innocence.

- *Cyber extortion*

More technical in nature than many of the other chapters, this chapter provides an example of an attempt to exploit weak security for profit. Rounding out the sequence of chapters related to forensics, this one provides the reader with effective techniques for investigation and actions taken toward ensuring usability of evidence.

Though no single text can supply all that one needs to form an effective security plan, *Defend IT: Security by Example* provides broad yet effective coverage of some of the most important elements. This book can be a very good place to start one's research into security planning, as well as a good refresher for experienced professionals.

Gary Dobbins (dobbins@nd.edu) is Director of Information Security at the University of Notre Dame in Indiana.