Introduction

Cybersecurity

Rick Kuhn, US National Institute of Standards and Technology

Enterprise security, often considered a burden for system administrators and users alike, is one of the most rapidly evolving areas of IT. This rapid evolution is a consequence of the high value of IT systems and the unending battle between attackers and defenders.

As with physical fortresses, advances by one side are met with subsequent advances by the other. In ancient times, defenders built stone walls; today, they build firewalls. Yet attackers have an extensive repertoire of methods for breaching both. Some techniques never change: ancient attackers sometimes had infiltrators within the fortress, or they'd trick defenders into letting them in. Today, insider threats and Trojan Horse programs remain two of the most serious IT security risks.

Ubiquitous Challenges

While the pattern of escalation between attackers and defenders remains constant, details obviously change very quickly. Changes in cybersecurity are driven from multiple sources:

- *Threat environment.* Both the number and magnitude of threats have grown substantially, from small-time criminals and intruders hacking for their own amusement to large-scale criminal enterprises. These enterprises attack millions of PCs for profit, seeking credit card numbers or other financially valuable information. Furthermore, with their increased scope, he skill level and resources available to attackers have grown as well.
- *Legal environment.* Along with this increase in attackers' sophistication, new laws and regulations in most nations have added to the need to protect privacy and security. What once might have been considered only good business practice might now be a legal requirement with substantial penalties should management fail to implement the necessary controls.
- *Technology environment.* No IT trend has attracted more attention in the past few years than cloud computing, which promises to change the delivery and use of information resources. This will remove many resources from locally managed systems to instead offer software as a service (SaaS). Simultaneously, smart phones with software applications provide specialized services nearly anywhere. Mark Weiser's prediction more than 20 years ago of ubiquitous computing has become a reality, but computing power everywhere brings with it an unavoidable need for ubiquitous computing security.

Clearly, today's enterprises have an opportunity to advance information security, but first they'll have to confront these problems.

Now more than ever, privacy and security aren't merely a burdensome but necessary part of IT systems operation—they can also contribute to the bottom line. The ubiquity of security challenges means that products and services that are more secure than their competition can have an edge in the market. This is particularly true with trends such as SaaS and cloud computing.

But for security to be a selling point, IT professionals must analyze and document information assurance features and practices, and customers must understand such features and practices.

In This Issue

The articles in this issue can help IT professionals who want to be intelligent providers or consumers of secure products and services.

"Anatomy of an Intrusion," by Shari Lawrence Pfleeger, is a fascinating case study of a sustained, sophisticated attack on a large multinational corporation. It provides a detailed look at the variety of methods attackers used to penetrate the organization's systems, how the attacks were discovered,

interactions with law enforcement, and ongoing actions by the corporation to prevent future penetrations.

"The Information Assurance Practices of Cloud-Computing Vendors," by Rajarshi Chakraborty, Srilakshmi Ramireddy, T.S. Raghu, and H. Raghav Rao, surveys security in the booming field of cloud computing. In addition to introducing the reader to information assurance in this relatively new field, it provides a framework for analyzing cloud vendor practices that readers can use when reviewing cloud services.

"Intrusion Detection for Grid and Cloud Computing," by Kleber Vieira, Alexandre Schulter, Carlos Becker Westphall, and Carla Merkle Westphall, describes an approach for detecting attackers in distributed systems—which can be even more challenging than detecting host-based intrusion.

In the Smart IT column, "Web Application Security: from Reactive to Proactive," John R. Maguire and H. Gilbert Miller explain how to break the "ignore-then-fix-it" cycle in Web application deployment. This cycle often develops when organizations rely too much on lower-level security and neglect application-level risks.

Finally, in this issue's Insecure IT column, Chris Johnson and I analyze data from the US National Vulnerability Database on software product vulnerabilities discovered in the past decade.

Software reliability, safety, and security all have something in common—the need for very high assurance. However, security is unique in that developers and operators are up against a human adversary working to overcome any mechanisms devised. Thus professionals must be aware of not only the latest developments in technology but also the methods available to adversaries. Hopefully this issue will help us all stay one step ahead of the bad guys.

Acknowledgments

I identify certain products here, but this doesn't imply recommendation by the US National Institute of Standards and Technology or other agencies of the US government, nor does it imply that the products identified are necessarily the best available.