Realtime
publishers

The Essentials Series:
Fulfilling Compliance by Eliminating Administrator Rights

Fulfilling Sarbanes-Oxley Compliance by Eliminating Administrator Rights

sponsored by
beyondtrust®

by Greg Shields

Fulfilling Sarbanes-Oxley Compliance by Eliminating Administrator Rights 1

Understanding Sarbanes-Oxley 1

SOX, Admin Rights, and the Goal of Least Privilege 3

Summary 4

Copyright Statement

Fulfilling Sarbanes-Oxley Compliance by Eliminating Administrator Rights

There's a problem with the widespread distribution of administrator rights in your organization, and it has nothing to do with security.

That problem is compliance: Compliance with the industry, governmental, and regulatory statutes that define certain configurations within your IT infrastructure. Although many of those configurations are mandated to enforce a greater level of security control, your job as IT professional is to ensure their fulfillment.

However, similar to the tradeoffs we endure between strong security and total usability, the solid implementation of a compliant configuration often requires a reduction in user flexibility, administrative capability, and merely getting the job of IT done. Nowhere is this more prevalent than in compliance's role in reducing the power and spread of administrative rights.

Understanding Sarbanes-Oxley

To begin, let's look at the regulations that make up the Sarbanes-Oxley (SOX) Act of 2002 itself. SOX was enacted by the United States Congress in response to a number of accounting scandals that occurred early in the decade. Its language implemented a set of requirements for financial reporting as well as corporate disclosure. Although the large majority of its guidance relates to business operations outside Information Technology (IT), some of its language has been interpreted to relate to the practices that IT uses in managing its information.

Of the major US compliance laws, SOX is considered exceptionally non-specific in terms of the guidance it provides to IT organizations. SOX mandates that a set of controls be put into place that manages the distribution and release of information. It further requires that provable auditing of those controls as well as their information under management is enabled at all levels.

There are four sections of SOX that are commonly scoped to include changes in IT practices, with one in particular having the most impact:

- **Section 302, Corporate Responsibility for Financial Reports.** This section requires that documentation of the company's operational activities and financial statements are certified by the company's CEO and CFO.
- **Section 404, Management Assessment of Internal Controls.** This section most relates to the operations of IT and requires that operational processes are documented. Further, all sources of data disclosed on financial documentation must be demonstrated. It is the interpretation of this section that mandates changes to IT's processes, requiring a greater level of control over IT data, privileges, and activity logging.
- **Section 409, Real-time Issuer Disclosures.** This section requires that changes in a company's financial condition or operations must be disclosed in real time to investors.
- **Section 802, Criminal Penalties for Altering Documents.** This section mandates the retention of certain documents using methods that cannot be altered. IT must ensure through some technical means that those documents have not been altered once created.

Unlike other compliance regulations—such as HIPAA for the healthcare industry, GLBA for financial services, and PCI for companies that store credit card information—SOX is not specifically limited to a particular industry. SOX's guidance relates to essentially any publicly-traded company. This means that organizations in one of these industries must often fulfill compliance from both their industry-specific regulations as well as SOX itself.

The operational realization of these regulations is generally accomplished through the correct assignment of user privileges as well as the monitoring of their activity. Thus, there must be an alignment between the job role requirements of users and the actual privileges those users are given. It also means that the activities of users on the network must be monitored with records of that activity being stored for later review. Further, those records must be stored in such a way that they cannot be erased or modified by an individual.

Ensuring SOX compliance is accomplished by proving that such controls are in place and that their auditing data remains unaltered.

SOX, Admin Rights, and the Goal of Least Privilege

That last statement—ensuring SOX compliance is accomplished by proving that such controls are in place and that their auditing data remains unaltered—is exceptionally important. IT organizations that fall under the rules of SOX must implement a set of "controls" that restrict the actions of users to just those tasks required by their job roles. Further, when users actually work with business systems, users' activities must be monitored and logged into a verifiable database. This task would be easy if it were natively supported by the Windows operating system (OS). To accomplish auditing on individuals' actions, many applications log information to Windows event log. However, if users have administrator rights, they can cover their tracks and erase the logs.

Although not explicitly stated, it is generally accepted that a central goal of SOX as well as every other industry, governmental, and regulatory compliance statute is the implementation of Least Privilege. The Principle of Least Privilege was developed more than 30 years ago by the United States Department of Defense (DoD). This principle "requires that each subject in a system be granted the most restrictive set of privileges…needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use."

By eliminating administrator privileges from your environment, you are moving that environment towards one that fulfills this principle's goals. You are at the same time going far towards fulfilling the requirements of regulations such as SOX.

Yet Least Privilege is more than simply eliminating administrator rights. Least Privilege can more broadly be described as the intersection of the user's role in the organization, the overarching corporate security policy of that organization, and the tasks that are available to be accomplished within the IT infrastructure. In effect, an environment that fulfills the requirements of Least Privilege will be very granularly capable of providing access to each person based on their needs.

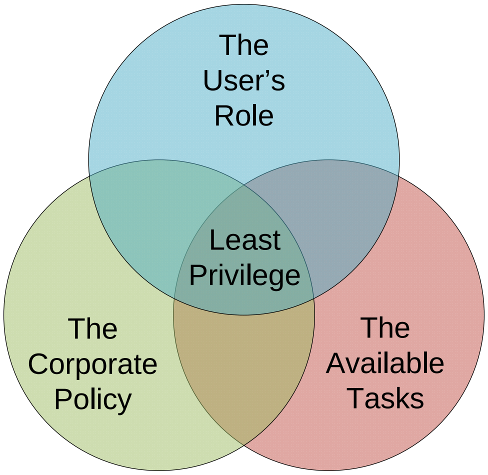

Figure 1: Least Privilege's elimination of administrator rights is really the combination of three factors.

For a comprehensive look at Least Principle's three overlapping requirements as well as how the effective elimination of administrator rights requires the involvement of each, check out *Essentials Series: Eliminating Administrator Rights*, found at http://www.beyondtrust.com/wp_ElimAdminRights_download.aspx?source=Realtime.

Unfortunately, the Microsoft Windows OS alone does not natively provide the architecture to enable this granular control. Using the Microsoft Windows OS, it is possible to eliminate the privileges assigned to an individual. However, these person-based privileges are far too coarse in their application. For example, with poorly-coded applications, simply removing administrator rights from a user may actually prevent needed applications from functioning. Other system configuration changes, like connecting to a local printer, can also require administrative rights, making their removal a problem for the user.

Summary

Organizations that fall under the scope of SOX should consider the use of external solutions that extend the granularity of privileges assigned. Such tools enable privileges to be assigned to applications based on user roles, adding that necessary granularity while still fulfilling the requirements of governmental mandates. These tools also provide the right level of audit-friendly logging that tracks user and administrator actions across systems, ensuring you meet your compliance regulations' requirements for activity tracking.