Realtime publishers

The Essentials Series:
Fulfilling Compliance by Eliminating Administrator Rights

Fulfilling PCI Compliance by Eliminating Administrator Rights

sponsored by

by Greg Shields

Copyright Statement

Fulfilling PCI 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 PCI DSS

Payment cards and the information they contain can be considered a direct linkage to a person's personal income. As such, the theft of that information is a major problem for consumers as well as the payment card industry in whole. The central problem with payment cards is that the information on their plastic is actually stored for periods of time on the computers of every storefront where they are used.

Because of this distribution of payment card data and the dangers it presents, in 2004, the major payment card companies—American Express, Discover, JCB, MasterCard, and Visa—agreed to create an industry standard that defined how payment card data would be secured. Describing specific requirements for data security in transit, during processing, and at rest, the Payment Card Industry Data Security Standard (PCI DSS) outlines explicit requirements for businesses that handle payment card information.

The compliance mandates required by PCI DSS are placed upon all industries that are involved with any form of payment transaction. This starts at the individual storefront or any institution that takes credit card payment, continues through the third-party processors that handle retail transactions, all the way through the banks that are responsible for the payments themselves. PCI DSS' regulations apply at every point during a payment card transaction's life cycle, and relate to any network component, server, or application that is included in or connected to the cardholder data environment.

The current PCI DSS version 1.2 is comprised of 12 high-level requirements that relate to six different goals. Each requirement has a number of sub-requirements that further outline its guidance. Specific details about those goals and requirements can be found at https://www.pcisecuritystandards.org/pdfs/pci_ssc_quick_guide.pdf. You'll quickly see in reviewing its goals that PCI DSS' guidance is fairly specific in relation to other industry and regulatory compliance guidelines currently in place today.

Although PCI DSS' requirements span the range of required security controls, a few relate specifically to the problems of administrator rights distribution:

- **Requirement #7.** In this requirement, businesses are instructed to restrict access to cardholder data by business need-to-know. Requirement 7.1 states that businesses should "Limit access to system components and cardholder data to only those individuals whose job requires such access." Requirement 7.2 continues with the need to "Establish an access control system for systems components with multiple users that restricts access based on a user's need-to-know, and is set to 'deny all' unless specifically allowed."

  The widespread distribution of administrator rights in an organization is at direct odds with these requirements. This is the case because administrator rights enable complete and unrestricted access to an entire system for the specified user. Thus, enabling administrator rights to those who do not require it for specific administrative actions specifically violates Requirement #7's guidance.

- **Requirement #8.** Some retail establishments historically created generic user accounts for all users of point-of-sale equipment. That practice over time found itself migrating into other areas of the network as well. This practice eases the use of these machines by retail employees but does not provide direct traceability between user and action. As such, no auditable logging of user actions can be done.

  To combat this shortcoming, users must be given specified accounts that are based on their person, and those accounts must be granted the granular permissions to accomplish the tasks associated with their job roles. Requirement #8 includes five sub-requirements that specifically define how this process should be accomplished.

- **Requirement #10.** Similar to the requirement for activity tracking in other compliance regulations, this requirement mandates that access and use of network resources is tracked. This tracking must be done across all accounts and should be protected against deletion. Requirement 10.1 states that businesses should "Establish a process for linking all access to system components to each individual user—especially access done with administrative privileges."

  Requirement 10.2 further mandates that businesses should "Implement automated audit trails for all system components for reconstructing these events: All individual user accesses to cardholder data; all actions taken by an individual with root or administrative privileges; access to all audit trails; invalid logical access attempts; use of identification and authentication mechanisms; initialization of audit logs; creation and deletion of system-level objects." As with other compliance regulations, these sub-requirements mandate that user and administration activities are tracked in an auditable way.

PCI DSS, Admin Rights, and the Goal of Least Privilege

Among other requirements, IT organizations that fall under the rules of PCI DSS are charged with implementing 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, their 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).

Although not explicitly stated, it is generally accepted that a central goal of PCI DSS 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 PCI DSS.

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.

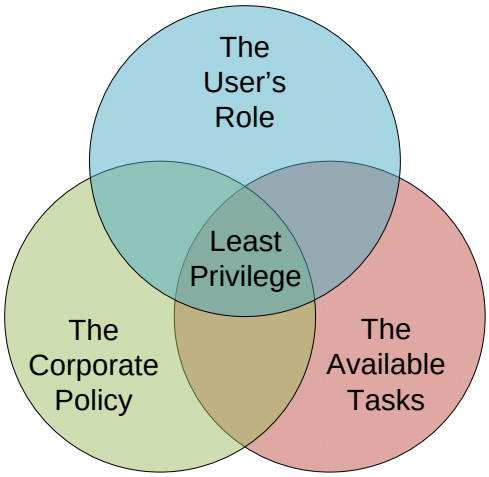

Figure 1: Least Privilege's elimination of administrator rights is really the combination of three factors.

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 PCI DSS 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.