Realtime publishers

The Essentials Series:
Fulfilling Compliance by Eliminating Administrator Rights

Fulfilling GLBA Compliance by Eliminating Administrator Rights

sponsored by
beyondtrust®

by Greg Shields

Copyright Statement

Fulfilling GLBA 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 GLBA

The Gramm-Leach-Bliley Financial Services Modernization Act (GLBA) of 1999 brought about a dramatic change in the way banks operate. The act was passed by the United States Congress to open up competition among banks, securities companies, and insurance companies by eliminating the previous rules that forced a separation between investment and commercial banks as well as between banks and insurers.

In addition to these large-scale changes to bank operations, two statutes focus on information security: the Financial Privacy Rule and the Safeguards Rule. The Financial Privacy Rule outlines guidance associated with the collection and disclosure of personal financial information for customers of financial institutions. This rule applies to both the financial organizations as well as any companies that receive this kind of information from financial organizations. GLBA's Safeguards Rule requires all financial institutions to design, implement, and maintain a set of safeguards that protect their customers' information. As with the Financial Privacy Rule, companies that receive this information are also responsible for these protections.

GLBA's guidelines are quite general in implementation, making them challenging to interpret and making difficult the task of designing solutions that comply with their mandates. Whereas other regulations such as PCI outline specific technical solutions or architectures that ensure security and protection, GLBA's guidance is at an extremely high level. GLBA's Privacy Rule includes language that:

- Requires the protection of an individual's personal information through the definition of privacy practices.
- Requires the creation of a privacy notice that explains those practices.
- Requires the distribution of that privacy notice on a yearly basis to customers and consumers of its services.
- Grants the ability for individuals to opt out of certain data-sharing arrangements that have been established by the financial institution. This can include limiting or blocking the transfer of information to non-affiliated companies.
- Prohibits the practice of "pretexting," which involves the collection of personal information under false pretenses.

These general guidelines are enforced through Title V of GLBA's implementing regulations—the "Safeguards Rule"—which states that:

> *Each bank shall implement a comprehensive written information security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the bank and the nature and scope of its activities…A bank's information security program shall be designed to:*
>
> 1. *Ensure the security and confidentiality of customer information;*
> 2. *Protect against any anticipated threats or hazards to the security or integrity of such records.*
> 3. *Protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.*

GLBA, Admin Rights, and the Goal of Least Privilege

You'll notice that nowhere in this guidance is any substantive detail about the technical solutions that should be implemented to fulfill these requirements. This specific guidance is left to the federal and state agencies that enforce its provisions. The result is that your auditing process for these regulations can be highly dependent on the agency performing the audit.

That being said, as with other compliance regulations, GLBA's guidance revolves around the protection of personal data through the implementation of technical controls. They also protect that data from corruption or change through established systems that enforce data integrity.

IT organizations are also 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 by auditors that a central goal of GLBA 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 GLBA.

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.

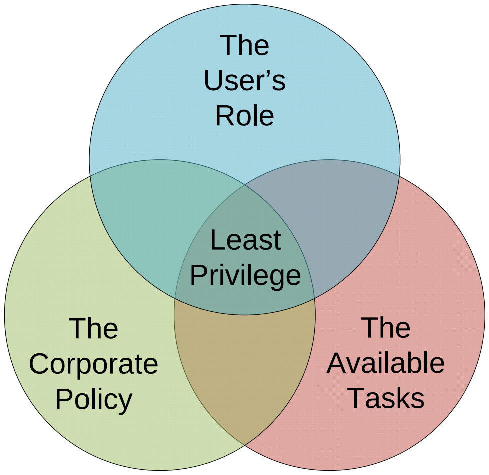

Figure 1: Least Privilege's elimination of administrator rights is really the combination of three factors.

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 GLBA 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.