WHITE PAPER

Three Pitfalls Of IT Security And How To Overcome Them

solarwinds

Introduction

Initiatives to improve IT security are often ineffective. The reasons for this can be summed up into three pitfalls: a one-sided perception of the threat, the implementation of initiatives with a rigid definition of security, and the downgrading of IT security to a corporate role.

This white paper will address an IT security framework created by SolarWinds that addresses these three pitfalls and introduces SolarWinds® Access Rights Manager (ARM).

PITFALL 1: A ONE-SIDED VIEW OF THE THREAT LEVEL

Discussions in the IT security sector currently tend to focus on new technologies and the risks from the professional hacking industry. Mobile end-user devices, cloud computing, and virtualization blur the boundaries between IT applications and corporate networks. Reports of spectacular cyberattacks on prominent institutions, such as on the banking, finance, healthcare and retail industries, as well as the reporting from prominent media companies, have primarily focused the discussion on external threats.

IT security against external threats is now indispensable for all industries and organizations. Nevertheless, this one-sided, outward-in view does not provide a complete picture of threats that organizations face. A simple mechanism is at work here: people tend to externalize security problems.

As a result, the walls protecting the organization's network from the outside are built ever higher, while the access within the network is often overlooked. "Insiders," who often move freely within a network, can be ignored, and many users end up with access to large quantities of knowledge and data. Databases and file servers may become exposed to unauthorized use, misuse, disclosure, destruction, or modification.

53% of surveyed organizations confirmed insider attacks in the previous 12 months, of which the main enabler was too many users with excessive access privileges.[1]

In addition to protections against external threats, it's critical that IT security also include the monitoring and controlled assignment of access rights based on the Principle of Least Privilege.

Principle of Least Privilege[2] *– provide access to only the information and resources that are necessary for its legitimate purposes.*

[1] Insider Threat 2018 Report, Cybersecurity Insiders, https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-report.pdf, accessed October 8, 2018.

[2] Applying the Principle of Least Privilege to User Accounts on Windows XP, https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-xp/bb456992(v=technet.10), accessed October 24, 2018

PITFALL 2: SECURITY MEASURES THAT SLOW DOWN WORK PROCESSES

Security initiatives are mostly well-intentioned, but still stumble over one main hurdle—they focus solely on increasing security. Security is, however, too abstract a concept in itself to provide recognizable value to the end user. IT security incidents, particularly within the network, are rarely identified, and thus remain beyond the experience of most employees.

IT security measures must also offer tangible benefits for users.

To make matters worse, interventions, the sole aim of which is to increase security, can limit the work processes of your users. This results in deviations from any new guidelines, which leads to the exact opposite of the desired results. The basic problem is that security and efficiency normally conflict with each other.

The sober realization remains that IT security measures must also offer tangible benefits for users. When this isn't the case, the intervention is unlikely to be accepted. It's therefore advisable to change the focus. The question is no longer primarily how to increase security, but rather, how to simplify existing security processes.

PITFALL 3: THE CENTRALIZATION OF SECURITY EXPERTISE

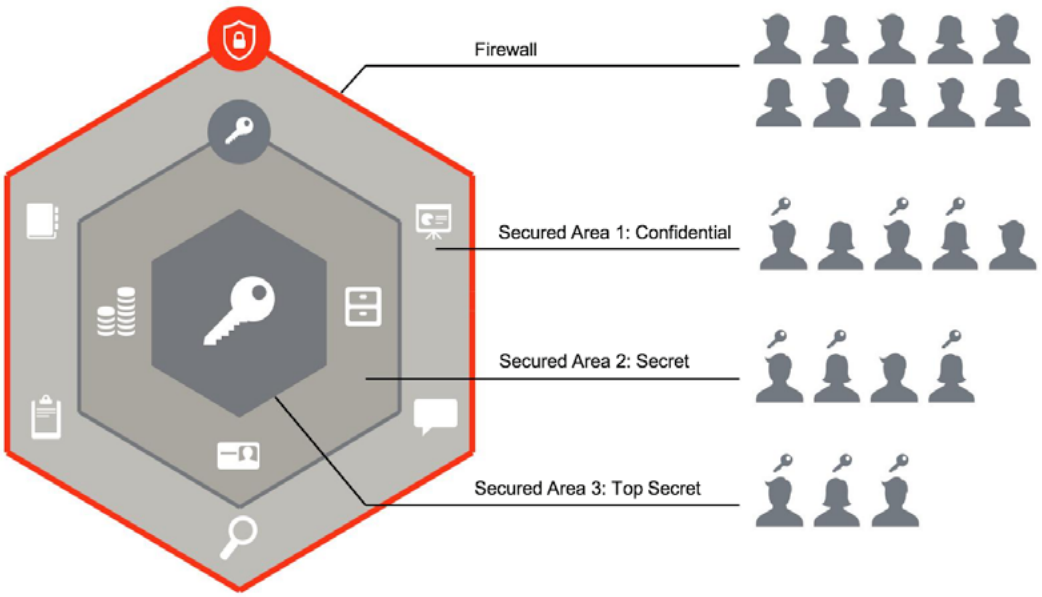
The increasing demand for IT security solutions has created a number of new roles: data privacy specialists, auditors, IT security managers, and information security managers who develop initiatives and monitoring tools to establish the foundation for greater IT security and data protection. This is a significant step from a business perspective. But many people are still under the illusion that their security issues are then fully resolved. Worse still, security expertise within the organization is often completely centralized within certain roles and restricted to these roles alone.

The problem with this is that security expertise cannot expand. Aspects of it should be developed in a decentralized manner within the organization, at least within senior management. The identification of sensitive information, knowledge, and data, and who should have access to these, can only be determined by the data owners within the different departments of an organization.

Without practical responsibilities tailored to the manager's working environment, any security initiative may be doomed to fail.

THE SOLARWINDS IT SECURITY FRAMEWORK

The SolarWinds framework grew out of the concept of giving IT security an inside-out focus and that the existence of protected areas within a network must also be ensured. These can only be created through different levels of confidentiality. Data, information, and knowledge are stored in different areas of the network. IT security starts with structuring and protecting content from inappropriate access.



The creation of protected areas within the network is a severely overlooked aspect of IT security. Why? Even for specialist administrators, it's difficult to protect the network from the inside. The analysis, documentation, monitoring, and changing of access rights are time-consuming activities and can pose significant IT problems.

When managing active directories, administrators should bear the group structures in mind, and assign access rights to File server, Exchange™, SharePoint™ and other resources to colleagues according to their roles. These rights are managed in different areas, which means that determining the current authorization status cannot be achieved efficiently and in a centralized manner. Nested group structures can only be unveiled by consolidating multiple sources.

The SolarWinds approach is problem-oriented towards simplifying security-relevant processes.

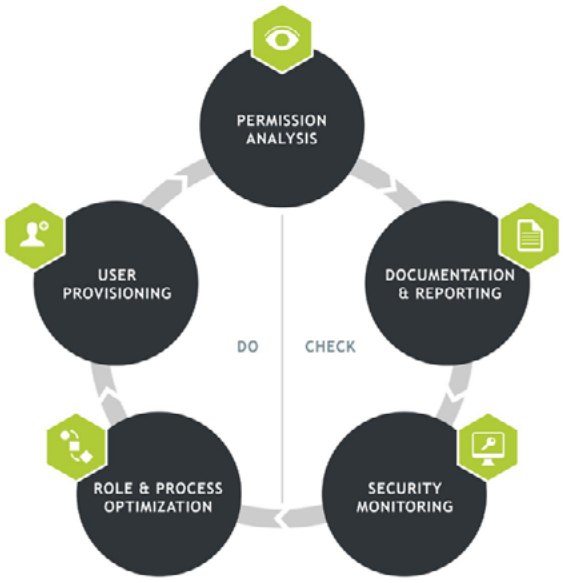
SOLARWINDS ACCESS RIGHTS MANAGER (ARM)

ARM is a powerful, affordable, and easy-to-use software solution that has been designed to help IT and security admins quickly analyze user authorizations and access permission to systems, data, and files, and help them protect their organizations from the risks of data loss and data breaches.

Simply put, ARM can help make user provisioning, deprovisioning, tracking, and monitoring easier, while minimizing exposure to insider threats

SolarWinds ARM establishes the basic conditions for the implementation of internal IT security with five basic services:

- Permission Analysis
- Documentation and Reporting
- Security Monitoring
- Role and Process Optimization
- User Provisioning



Permission Analysis allows administrators to determine the access rights situation within the network for the first time for all resources. ARM provides a central view of group memberships from the Active Directory®, as well as File server and Exchange access rights. This knowledge is a prerequisite for identifying security gaps and taking appropriate measures.

Managers spend a lot of time on documentation in order to fulfill the requirements of IT security, statutory regulations, and audit. The **Documentation and Reporting** service focuses on this obstacle. Visible access rights histories, and reports can be generated with only a few clicks. These can be sent automatically to senior management, IT managers, data privacy specialists, and auditors.

The traditional analysis of access rights is limited to determining the current access rights situation. ARM **Security Monitoring** allows the detection of all security-relevant activities on the network and file servers. This closes a major security loophole: self-assigned access rights intended for data theft no longer fly under the radar. Moreover, particularly sensitive, security-relevant directories are monitored on a permanent basis on the file server, down to the individual file level.

With ARM, internal security is no longer merely a policy on paper. It allows data owners to be nominated for each area. These then use a simple interface to assign access rights for their users, and they can also create protected directories for sensitive knowledge on the file server. Administrators are no longer part of the process and can focus on their own projects.

ARM decentralizes security and contributes to security awareness within the business.

User Provisioning covers the setup of new user accounts, rights management, and the editing of account details. All of these tasks can be performed in ARM by different roles and through one system, thus preventing media disruptions or other consequences. Standard tasks, such as the user setup and account management, can be delegated to the help desk.

SEE HOW SOLARWINDS ACCESS RIGHTS MANAGER WORKS IN YOUR ENVIRONMENT

It's easy to see just what ARM can do for you. Simply download a free 30-day trial or give us a call and one of our specialists will arrange a personalized demo.