8MAN

Access Rights Management. Only much Smarter.

THE THREE PITFALLS OF IT SECURITY

Protected Networks

IT SECURITY IN FOCUS

THE THREE PITFALLS OF IT SECURITY AND HOW TO OVERCOME THEM

Abstract:

Initiatives to improve IT security are often ineffective. The reasons for this can be summed up in 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.

The 8MAN access rights management solution is a good example of how to avoid these pitfalls, which is why it has become a widely accepted and practical security solution.

1. THE THREE PITFALLS OF IT SECURITY

1.1. A one-sided view of the threat level

Discussions in the IT security sector are currently focused on new technologies and the risks from the professional hacking industry. These two issues are interconnected. Mobile end-user devices, cloud computing and virtualization are blurring the boundaries between IT applications and corporate networks. Reports of spectacular cyber-attacks on prominent institutions, such as on the banking, finance, healthcare and retail, as well as the reporting from prominent media companies, have focused the discussion on external threats.

IT security against external threats is now indispensable for all industries and orgnaizations. Nevertheless, this one-sided outward-facing view is deceptive. It is the result of realistic threats, but is also powerfully influenced by media reporting. A simple mechanism is at work here: People tend to externalize security problems.
As a result the walls protecting the corporate network are built ever higher, and the boundaries of areas within the network are overlooked. "Insiders", who often move freely within a corporate network, are ignored. This means that many employees have access to large quantities of knowledge and data. This creates security risks: Customer data, projects and prototypes are uncontrollably laid open and can be copied undetected.

> „55 percent of security attacks originate from data thieves with access rights."

The big issue: According to the IBM Cyber Security Intelligence Index, 55 percent of security attacks originate from data thieves with access rights.
In addition to protections against external threats, such as firewalls, the basics of IT security also include the monitoring and controlled assignment of access rights.

1.2. 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 company network, are rarely identified and thus remain beyond the experience of most employees.

To make matters worse, interventions whose sole aim is to increase security limit the work processes of your employees. This results in deviations from any new guidelines, which leads to the exact opposite of the desired results. Basically, the problem is that security and efficiency are normally at loggerheads with each other.

> „IT security measures must also offer tangible benefits for users."

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

1.3. 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 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 company 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 must be developed in a decentralized manner within the company, at least within senior management. The identification of sensitive information, knowledge and data and who should have access to these can only be determined within the different departments of a company.

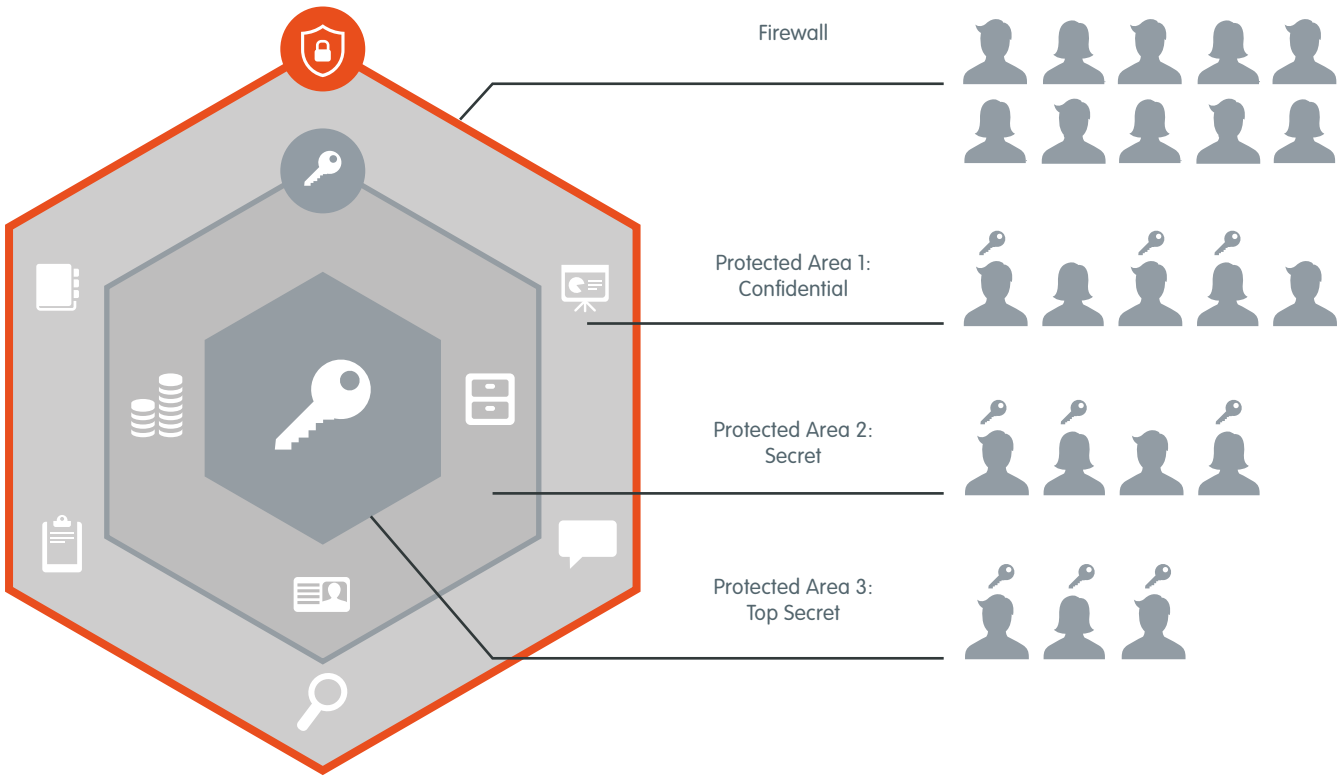
In conclusion:

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

2. THE 8MAN IT SECURITY CONCEPT

8MAN grew out of the concept of giving IT security an inward focus. The firewall is only the first barrier.

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

When managing active directories, administrators must bear the group structures in mind, and assign access rights to Fileserver, SharePoint, vSphere, Exchange 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.

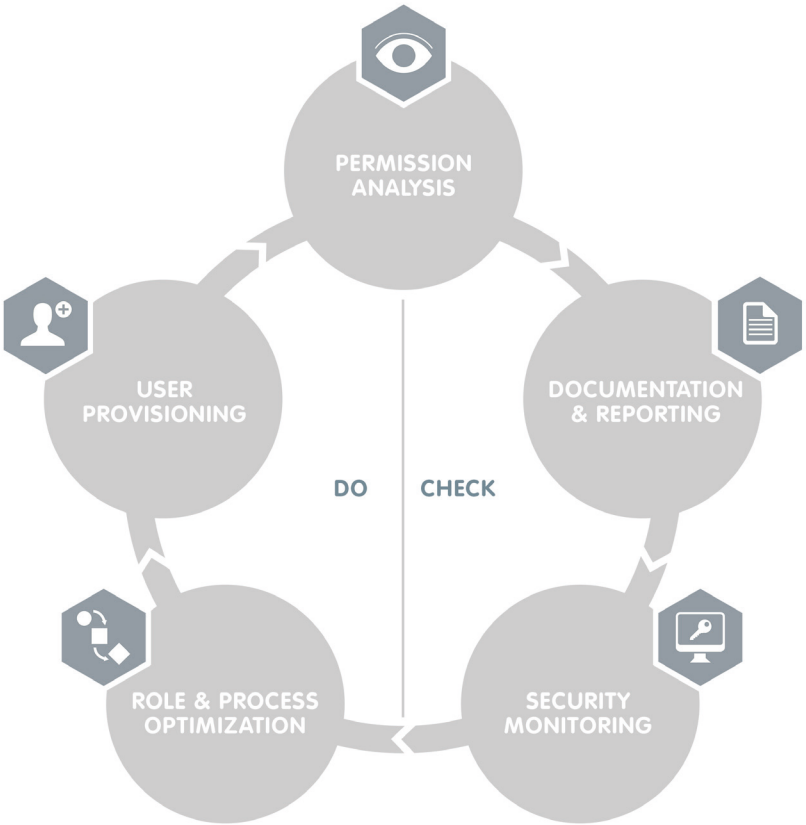
„The 8MAN approach is problem-oriented towards simplifying security-relevant processes."

The 8MAN approach is problem-oriented focusing on simplifying security-relevant processes. Only then can their implementation be guaranteed. 8MAN establishes the basic conditions for the implementation of internal IT security with five basic services - Permission Analysis, Documentation & Reporting, Security Monitoring, Role & Process Optimization and User Provisioning.

2.1 Access rights management as a basis for IT security

Permission Analysis allows administrators to determine the access rights situation within the company network for the first time for all resources. 8MAN provides a central view of group memberships from the Active Directory as well as Fileserver, Sharepoint Sites, Exchange and vSphere 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 fulfil the requirements of IT security, statutory regulations and audit. The **Documentation & Reporting** service focuses on this obstacle. Visible access rights histories and audit-proof 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. 8MAN **Security Monitoring** allows the detection of all security-relevant activities on the company's network and files 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.

Security affects us all. It is far too important to be completely centralized. For this reason, 8MAN has established a data owner concept with Role & Process Optimization. Data owners are managers and are structurally deemed to be the most appropriate decision-makers when it comes to the assessment and classification of sensitive knowledge. Moreover, as the direct interface to their employees, they are in a position to decide who should have access to what.

With 8MAN, 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 employees, and they can also create protected directories for sensitive knowledge on the file server.

„8MAN decentralizes security and contributes to security awareness within the business."

8MAN decentralizes security and, by assigning responsibility to data owners, contributes to security awareness within the business. Administrators are no longer part of the process and can focus on their own projects.

"User Provisioning" covers the set-up of new user accounts, rights management and the editing of account details. All of these tasks can be performed in 8MAN by different roles and through one system thus preventing media disruptions or other consquences. Standard tasks such as the user set-up and account management can be delegated to the Helpdesk.

2.2 Security works efficiently: How to secure your business

Introducing 8MAN is not a project in itself: All it takes is a phone call. Arrange an appointment and a certified technician will do the installation and configuration in your company. Depending on the options in your company, the installation can also be carried out completely via remote access.

Scheudle a Demonstration

Start with a 30 minute tour and see 8MAN in action. Participants remain anonymous. At the end of the presentation, you will have the opportunity to ask questions in a chat session.

Test drive it with a self-guided demo

Contact

Address:
Protected Networks GmbH,
Alt-Moabit 73,
10555 Berlin,
Germany

Website:
http://www.8man.com

E-Mail:
info@8man.com

Author:
Fabian Fischer
Knowledge Manager | 8MAN