SSE® Network Services

70% of Security threats Originate Inside Your Office

By Elizabeth Elliott
Niedringhaus
President and CEO of SSE

Are Your Employees Stealing Inside Information?

External menaces like viruses and spyware are not the only threats to your computer. Threats from internal sources can also cause dramatic problems. Trusted inside sources generate more than 70 percent of unauthorized data access, according to Gartner, the world's leading provider of research and analysis of the global IT industry.

Companies typically focus on protecting their businesses from external threats by deploying firewalls, anti-virus software and/or intrusion detection systems. While these are critical, they offer little to no protection against surreptitious actions by such internal sources as employees, partners, contractors and customers.

Data Access Control Without data access control, any internal source is free to access, copy, change or delete data. Users can open an email account with an external provider and use high-speed Internet connections to simply email key data to their personal accounts, bypassing any corporate email system. Thumb-size USB hard drives contain sufficient space to copy thousands of internal documents in minutes.

To protect your corporate data, you must establish adequate data access controls. The first step is to categorize the types of data requiring security. For example, in the accounting department, two or more groups may be appropriate, such as Accounts Payable and Accounts Receivable. The system can be configured to give members of the Accounts Payable Group “read and write” access while automatically prohibiting access to non-members. After all groups have been defined and appropriate security rights assigned, make each employee a member of the groups where access is required. As employees are hired or depart, promptly add or remove membership.

Auditing & Passwords The second step is to enable account auditing and implement a secure password policy. Auditing will log all successful and failed user access attempts. Password policy works to enforce safe standards. Insist on password complexity, requiring a combination of letters, numbers and non-alphabetic characters (e.g. P@ssword1). Require passwords of eight characters and regular password changes. Enforce automatic system lockout for any login attempts that fail three or more times to protect against brute force access attempts. Finally, audit your system with a third-party tool to verify compliance.

If you are a business owner who is overwhelmed by the requirements of maintaining your computer systems and protecting your operations, call on SSE today for assistance. Schedule your FREE IT Security Audit today, and ensure the safety of your computer network.

SSE Network Services Division
www.SSEnetwork.com

With our proprietary managed service solution, Pretecht^{sm}, SSE can efficiently manage your IT services so you can effectively manage your business! Outsourced with SSE, Consider I.T. Done^{sm}!

PRETECHT
Pretecht by SSE
314-439-4700