Security and privacy in the network context

Sociology

The other technique is to recognize potential vulnerabilities and suggest remedial actions to secure a database system. ISS Database Scanner Software, a product available with Oracle, Microsoft SQL Server and Sybase databases automatically scrutinizes the system for insubstantial passwords and viruses.

A more intricate database security device is presented by Guardent through its Security Management Appliance. It works behind a firewall and remotely detects vulnerabilities. It covers operating systems, applications and network infrastructures, and remote online databases.

Experiences and experts analysis dictates that more responsive social and organizational actions should be taken. Accounting for the losses in businesses and the effects in the economy, protecting databases from hackers is now a serious business.

Our society and organization should be vigilant in protecting our vital and key information against criminal elements using the technology to spy, steal and destroy our investments. We must first ensure that our network security is reliable and constantly updated. Let us remember that nowadays, spending a little more on security software even for personal use is fundamental.

Invest in reliable and tested database applications; buy only those programs with robust security design. For companies, ensure that personnel in the system administration are strictly following security guidelines. Apply more restrictions to database access especially on internet-based databases that are more vulnerable to attacks. Configure your server to allow only those trusted IP addresses and employ Table Access Control security on your databases.

Long-Term Network and Data Security, and Privacy Rights

There are many ways to secure access to vital information in a Network, Database, and Individual Private files. At present, Operating Systems and Database Systems come with security features that can considerably prevent unauthorized access.

Long-term methods are available from various reputable computer security companies such as Servers employing Trusted IP Address methods. This is done by configuring the server access to a list of " trusted" users only. Next is Server Account Disabling which suspends the server ID after three unsuccessful attempts. This is done to prevent attackers from generating random passwords to get the right combination. Monitor the system; get a product that would send an alert when someone wants to break-in into the system.

Secure the system with authentication methods such as Kerberos Security, a " ticket" based authentication systems from Oracle (Weidman, n, d.). Restrict access to selected rows of databases by employing VPD (Virtual Private Database) Technology.