

Database Security Notes

The Levels of DB Security

Database Level – database users and authorization

Application Level – information management and processing

Operating System Level – data storage and protection

Network Level – data transmission

Physical Level – computer equipment protection

Human Level – social engineering protection

Database Level Security

- Database Privileges
 - Read – read, but not modify
 - Insert – add new, but no changes
 - Update – modify, but no delete
 - References – allowed to create foreign keys
 - Delete – delete rows
 - Index – create and delete indices – structure for performance enhancing
 - Resources – create relations
 - Alteration – add or delete attributes
 - Drop – delete relations
 - Grant – ability to grant privileges
- Encryption of actual data is good, but not enough
- Only grant enough privileges to a user to allow them to do their job
- Create admin users for admin duties, application users for each application

Application Security

- Write programs with security in mind from the beginning!
- Strong typing of applications to prevent type errors!
- Catch and handle all errors!
- Encrypt data when possible! Don't use open channels through the application!
- Tunneling using SSH

OS Security

- Virus protection and firewalls
- “Wizards” are bad. Don't be a novice doing this! SQLServer – if you just click through the installation, use “sa” with no password is created! Free superuser!
- File system issues – can get to the actual bits, they can get the actual data – remember, mysql is just a bunch of files in a directory!
- Hide stuff! Lock down your machine itself! Protect it!
- Don't install adware or spyware!
- Run a minimal set of programs! You open more doors if you don't! Disable all extra programs!
- Close all ports! Lock down the interfaces

Network Security

- Hide the server! Don't make it world visible!
- Don't make your database server your web server!
- "You can't access what you can't see!"
- Limit connections to DB server only from trusted sources (like the web server) PostgreSQL does this well. Setting where you specify IP's, mac's etc.
- Change your default port!
- Separate server for authentication!
- Firewalls!

Physical Security

- Lock the door; lock the box; lock the backups
- Hide the keyboard; hide the mouse; hide the monitor; hide the plugs
- Use a locked cabinet in a locked room
- Use a UPS

Human Security

- An estimated 70% of unauthorized access to information is committed by internal employees — who are also responsible for more than 95% of intrusions that result in significant financial losses.
- Know who you give rights too
- Hire good people
- Pay well at the company so they aren't susceptible to bribes
- Never give out your password
- Do training about password scams (this email is from tech support... etc.)
- Do training about viruses and how to handle your computer
- Log off at lunch
- Never bring software from home to put on at work
- Explain policies for not following rules and enforce them

Other things to consider:

- A uniform approach to security across computer systems and databases
- Identification of the form and style of authorization required to initiate the creation of an account
- A determination of who will create user accounts on the operating system, within each application if necessary, and within the databases
- How those accounts will be created
- Whether a standard convention for usernames and passwords should be imposed and what it should be
- Whether password aging will be enabled and in what time frame
- A determination of access requirements on an application-by-application basis
- Identification of how users will be tracked to ensure that as an employee's job description or location changes, the access to applications remains correct
- Identification of sensitive information and an outline of steps to take for data protection
- A determination of penalties to be enforced as a result of different levels of security breaches