

DATABASE BY DESIGN, INC.

Database Security

Keeping your clients informed without breaching security

Are your customers and business partners asking you to conduct transactions online? Are you hesitant because you are concerned about the security of your information? You aren't alone. Statistics such as the following would give anyone reason to pause:

"Internet attacks against public and private organizations rose by 28 percent in the first six months of 2002, reports TechNews. ...according to a new industry report from Ripstech...cyber-security breaches at more than 400 organizations revealed evidence of over 180,000 successful Internet attacks from January to June."¹

After noting the reports of security breaches in the news, it may seem risky to put your valuable and confidential information on the web. However, by understanding basic security risks you can implement measures to thwart attempts by unauthorized people to get to your data.

What Are the Risks?

Hacking - This term refers to the process of breaking into a system by systematically guessing at passwords or looking for unguarded 'back doors'. A 'back door' is a method of getting to your online data without going through the normal security processes. These are established by your system administrator 'just in case there is a problem' or because administrators don't want to be bothered with tight security. Hackers try to find these 'back doors' and use them to get in. Also, they try to figure out how you have set up the system. A successful hacker is hoping that you set your system up the same way that everyone else does.



Software Holes - Hackers often get help from the very software they are trying to break. Holes in the form of bugs or vulnerabilities in software can be exploited by hackers to gain access to your server. Some bugs cause minor annoyances. However, other bugs can compromise your system and allow unauthorized access to all of your data!

Disgruntled Employees - An often overlooked area of security involves people within your own organization. Most breaches in security result from employees or former employees accessing systems with the passwords given to them.

"...a survey by security software developer Camelot and eWEEK found most security breaches originate in-house. The survey found that authorized users, such as employees, contractors and consultants, commit the majority of security breaches at companies.

Among the findings of the Camelot/eWEEK survey:

57 percent of respondents cited users accessing resources they shouldn't be entitled to as a cause of network security breaches

43 percent of respondents indicated security breaches were caused by user accounts left open after an employee has left the company"²

Security Checklist

Now that the trouble spots are known, you can take steps to keep your data secure. The following is a checklist that you can use to help stay on top of your security measures:

- Keep your 'back doors' closed.** If you must have a way into your system that isn't the normal route, make sure the security used here is as good or better than the rest of the system.
- Don't use the standard setup for online software.** Many web based software programs are installed with most of the access options turned "on". This gives hackers plenty of opportunities to try several of their secrets. Make sure that the software that you have installed only has active features that are necessary for your particular system. Outsourcing with a software professional is a good way to ensure that your software doesn't have any unplanned openings.
- Keep your software patched.** No software is perfect. Even the best of software has occasional bugs that can compromise the security of your online system. Fortunately, patches to the software are often available before the bug becomes widely known. Having your software patched in a timely manner can increase the security of a system. Contracting with a software professional for this item can be very cost effective.
- Don't use easy to remember passwords.** Dates, names of pets, and other easy to remember passwords make it too simple for hackers and disgruntled employees to gain access. Use passwords that have letters and numbers combined which don't make normal words.
- Change your passwords.** Changing your passwords occasionally makes it hard for someone to guess at it over time. Also, if you ever have staff changes, make sure to change everyone's passwords immediately.
- Encrypt your sensitive data.** If your online system contains sensitive information, such as credit card numbers, have your database program store the information in an encrypted format. Encrypting is a method of applying a formula to information that makes it impossible to be read without the proper encryption 'key'. Security measures of this type are extremely effective. That way, even if there is unauthorized access to the data, the person won't be able to use it.



Putting your organization's information online for your customers and business partners can have significant advantages. Make sure that the information is well protected so that it continues to be an asset instead of a liability. At Database by Design, Inc., we consider the safety of your online information a major factor of the success of your Internet enabled database system. Contact us so we can help you address the security needs of your database programs!

Database by Design, Inc. - (503) 579-4638
info@mycustomdatabase.com
<http://www.mycustomdatabase.com>
http://www.mycustomdatabase.com/newsletter_archives.html
(Previous Newsletters)

Next Month's Topic: To fix or re-build? When is your database past its prime?

References

- ¹ “Worldwide cyber-security breaches on the up”,
http://www.nua.ie/surveys/?f=VS&art_id=905358144&rel=true.
- ² “Internal Threats Justify Increase in Security Spending”,
http://cyberatlas.internet.com/big_picture/applications/article/0,,1301_787251,00.html.