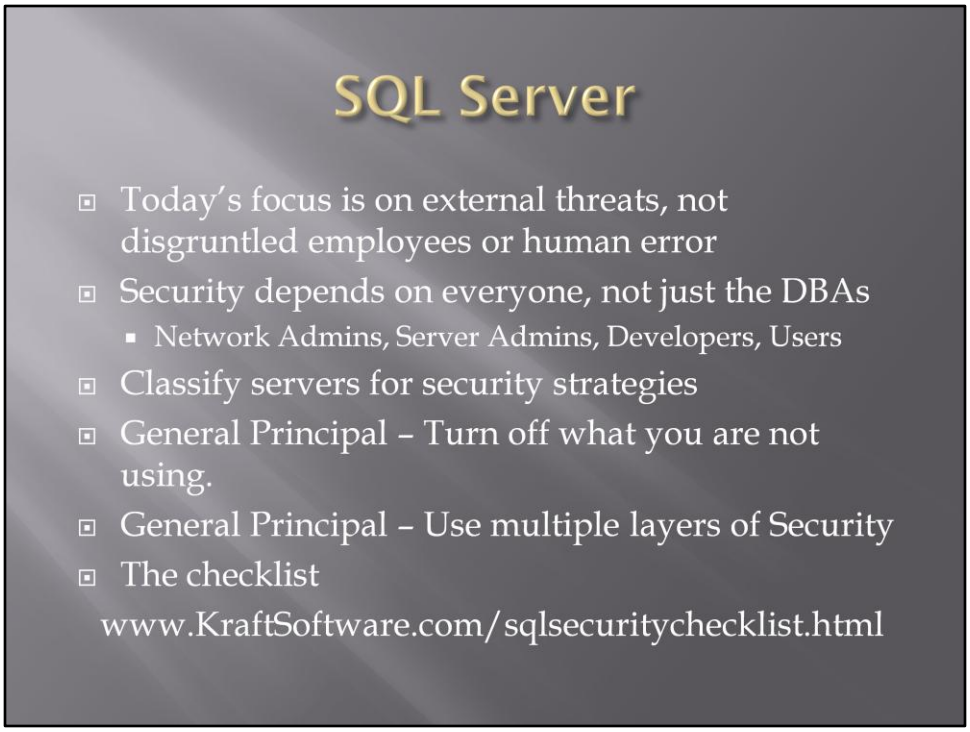
SQL SERVER SECURITY

All Things Considered

Rob Kraft
www.KraftSoftware.com

Today we are going to focus on SQL Server, but a more complete security assessment would start with Threat Modeling. Threat Modeling is a process used to identify what assets you have that need to be secured, identifying the security risks to each asset, and developing plans to mitigate those risks.

When you are evaluating actions to be taken to improve the security of SQL Server, you should also identify compliance needs, the performance impact of possible courses of actions, and your recoverability needs. Implementing certain security measures could negatively impact performance and complicate backup and recovery scenarios. Therefore you need to consider other factors before making changes solely for the sake of security.



Many of the tasks necessary to hardening (implementing good security policies) a SQL Server are not DBA tasks.

If you desire to develop a set of policies that apply to all SQL Servers, you should plan to develop two or three policy sets, then apply the appropriate set of policies to each SQL Server. Production servers full of credit card numbers may need different policies than the SQL Express instance for the developer of blog application. The two or three classifications you use for SQL Server policy groups will probably also affect your auditing policies for those SQL Server as well as your update policies and backup strategies.

Turn off what you are not using. One change I recently made for a client was to turn off the wireless access to the router that no one (that they knew of) was using.

You may suspect that some security recommendations provide very little additional security, and in some cases that is true. But that little bit of additional security may be the very thing that keeps your SQL Server from getting compromised. You should not rely on just one, two, or three barriers to protect your data, especially when additional barriers are easy to erect. Each security feature you add reduces, at least a little, the risk of being hacked.