BUILD ON

MICROSOFT INFORMATION SECURITY

ACE SERVICES

Application Security Design Review

The Microsoft Threat Modeling methodology objectively and consistently identifies threats, thereby enabling the creation of a security strategy.

The Microsoft Information Security ACE Services team has over 8 years of experience in protecting Microsoft's own assets at Microsoft IT

The Application Security Design Review service provides you with data that will help you understand potential threats to your mission-critical applications and the steps needed in order to mitigate risk associated with each threat.

Microsoft will perform a careful examination of your application design, looking for weaknesses in the design choices and implementation. By engaging Microsoft to perform a security design review of your mission-critical applications, you reduce the risk of financial loss, as well as asymmetrical risk to reputation at the hands of malicious hackers.

What happens in a Security Design Review?

A time tested approach to secure system design, known as Threat Modeling is applied to identify and enumerate threats. Microsoft has pioneered the approach and created significant intellectual property in terms of tools and knowledge gained while protecting its own assets. The same knowledge and tools are applied to your application.

Typically a system walkthrough is scheduled with your team, followed by a documentation review of the system design. The system is then analyzed using the threat modeling framework such as STRIDE or others as appropriate to list potential scenarios under which various threats may materialize.

.

You receive a detailed report allowing your team to focus on the right aspects of your security at the right time

When to perform a Security Design Review?

In general, a security design review can be performed at any time in application lifecycle management cycle as long as the design of the application is feature complete. However, the best time to perform a security design review is when the application team has just finished the design phase and the next milestone in software development lifecycle is code building. During this time, the development team can use the knowledge gained via the security design review to protect the application before the application teams start coding.

Deliverables

The deliverable consists of a highly detailed document indentifying all potential threats uncovered by the design review. A risk rank is assigned to each threat, which allows your team to focus on the right thing at the right time.

After completing the security design review, Microsoft experts will:

- Rationalize threat levels with your team.
- Provide guidance on mitigating the threats.

Return on Investment and Cost Benefit

Several reasons contribute to the return on investment argument, however the most significant of those are

1. Reduce the cost of fixing the system design by performing a review before application goes into coding.
2. Reduce the probability of getting attacked from inside and outside the perimeter.
    a. Protect your brand name
    b. Protect your data

Additional Offerings

Prior to a security design review:

- Custom Secure Design Guidance Engagement
- Secure Application Development Training.

Post security design review:

- Security Code Review
- Custom Server Hardening Engagement

For more information
Contact your Microsoft Services representative or visit www.microsoft.com/services.