Risco

Riscos de Segurança em Risco Aplicações

**O que são Riscos de Segurança em Aplicações?**

Os atacantes podem, potencialmente, usar vários caminhos diferentes através da aplicação para causar danos ao negócio ou organização. Cada um desses caminhos representa um risco que pode, ou não, ser grave o suficiente para que se justifique uma chamada de atenção.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Agentes de Ameaça | Vetores de Ataque | Vulnerabilidades de Segurança | Controlos de Segurança | Impactos Técnicos | Impactos no Negócio |
|  | Ataque | Vulnerabilidade | Controlo | Ativo | Impacto |
| Função |
| Ativo |

Por vezes, é trivial encontrar e explorer esses caminhos, e por outras vezes, é extremamente difícil. Da mesma forma, o dano causado pode não ter consequências, ou pode acabar com o seu negócio. Para determinar o risco para a sua organização, pode-se avaliar a probabilidade associada a cada agente de ameaça, vetor de ataque, vulnerabilidade de segurança e combiná- la com uma estimativa dos impactos técnico e no negócio da sua empresa. Juntos, esses fatores determinam o risco total.

**Qual é o Meu Risco?**

O OWASP Top 10 foca-se na identificação dos riscos mais graves para uma ampla gama de organizações. Para cada um destes riscos, fornecemos informações genéricas sobre a probabilidade de ocorrência e impacto técnico usando o esquema simples de classificação abaixo, que se baseia na metodologia de avaliação de riscos da OWASP (OWASP Risk Rating Methodology).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Agentes de Ameaça | Vetores de Ataque | Prevalência da Vulnerabilidade | Detecção Vulnerabilidade | Impactos Técnicos | Impactos no Negócio |
| Específico da Aplicação | Fácil | Generalizada | Fácil | Severo | Específico do Negócio/ Aplicação |
| Média | Comum | Média | Moderado |
| Difícil | Rara | Difícil | Pequeno |

Somente você saberá os detalhes do seu ambiente e do seu negócio. Para qualquer aplicação, pode não haver um agente de ameaça que possa executar um ataque relevante, ou o impacto técnico poderá não fazer nenhuma diferença para o seu negócio. Portanto, deve-se avaliar cada risco, focando-se nos agentes de ameaça, controlos de segurança e impactos no negócio de sua empresa. Nós listamos quais os Agentes de Ameaça como sendo Específicos da Aplicação, e os Impactos no Negócio como Específicos do Negócio/Aplicação para indicar que estes são claramente dependentes dos detalhes sobre a aplicação na sua empresa. Os nomes dos riscos no Top 10 derivam-se do tipo de ataque, do tipo de vulnerabilidade, ou do tipo de impacto causado. Escolhemos nomes que refletem com precisão os riscos e, quando possível, alinham-se com a terminologia mais provável para auxiliar na conscientização das pessoas.

**Referências**

**OWASP**

• OWASP Risk Rating Methodology

• Article on Threat/Risk Modeling

**External**

• FAIR Information Risk Framework

• Microsoft Threat Modeling (STRIDE and DREAD)