## NIST SP 800-30 Rev. 1

## 

### **Guia para avaliação de risco**

O NIST SP 800-30 é uma publicação que fornece orientação sobre a realização de avaliações de risco. Ele descreve estratégias para identificar, analisar e remediar riscos. As organizações usam o NIST SP 800-30 para obter insights sobre a probabilidade e a gravidade potenciais dos riscos, ajudando-as a tomar decisões informadas sobre alocação de recursos, implementação de controles e priorização de esforços de remediação.

Este documento de quatro páginas é adaptado do NIST SP 800-30 Rev. 1. O termo "Rev. 1" significa que é a primeira versão atualizada desta publicação. O NIST ocasionalmente revisa seus documentos para incorporar novas informações, refletir mudanças na tecnologia e nos requisitos regulatórios ou abordar feedback.

Observação: o Computer Security Resources Center do NIST contém mais informações sobre o SP 800-30 Rev. 1.

### **Fontes de ameaça**

O NIST SP 800-30 define e categoriza fontes de ameaças como entidades ou circunstâncias que podem impactar negativamente os sistemas de informação de uma organização. Essas informações são úteis para identificar e avaliar riscos potenciais. Ao referenciá-las, considere a intenção/capacidades de fontes de ameaças internas e externas.

Nota: A tabela a seguir lista algumas possíveis fontes de ameaças que podem comprometer um servidor de banco de dados acessível publicamente.

|  |  |  |
| --- | --- | --- |
| Tipo | Exemplos | Descrição |
|  | *Usuário padrão*  *● Funcionário*  *● Cliente*  *Usuário privilegiado*  *● Administrador do sistema*  *Grupo*  *● Concorrente*  *● Fornecedor*  *● Parceiro de negócios*  *● Estado-nação*  *Outsider*  *● Hacker*  *● Hacktivista*  *● Ameaça persistente avançada (APT)* | Ameaças que surgem de indivíduos ou grupos que podem explorar recursos cibernéticos propositalmente ou acidentalmente. Por exemplo, eles podem alterar dados de uma forma que impacte negativamente a empresa. Alternativamente, eles podem intencionalmente roubar dados e danificar equipamentos comerciais. |
|  | *Hardware*  *● Armazenamento*  *● Processamento*  *● Comunicações*  *Software*  *● Sistema(s) operacional(ais)*  *● Rede*  *● Software malicioso* | Ameaças que se originam de fatores não humanos. Por exemplo, falhas de equipamentos devido ao envelhecimento, esgotamento de recursos ou outras circunstâncias. |
| **Environmental** | *Ambiente operacional*  *● Controles de temperatura*  *● Controles de umidade*  *● Fontes de alimentação defeituosas*  *Riscos naturais*  *● Quedas de energia*  *● Eventos climáticos extremos* | Ameaças que surgem de fatores acidentais, não humanos. Por exemplo, falhas de equipamento causadas pelo ambiente operacional. |

### **Eventos de ameaça**

O NIST SP 800-30 define e categoriza eventos de ameaça como instâncias reais em que uma fonte de ameaça explora uma vulnerabilidade e causa danos ou prejuízos aos sistemas de informação de uma organização. Essas informações são úteis para obter insights sobre os tipos de riscos que os ativos enfrentam. Controles e contramedidas mais eficazes podem ser identificados ao entender possíveis eventos de ameaça,

Observação: a tabela a seguir lista apenas alguns possíveis eventos de ameaça que podem comprometer um servidor de banco de dados acessível publicamente.

|  |  |
| --- | --- |
| **Exemplos** | **Descrção** |
| Realizar reconhecimento e vigilância da organização | A fonte da ameaça examina e avalia as vulnerabilidades da empresa ao longo do tempo usando várias ferramentas (por exemplo, varredura, observação física). |
| Obter informações confidenciais por meio de exfiltração | A fonte da ameaça instala software malicioso em sistemas organizacionais para localizar e adquirir informações confidenciais. |
| Alterar/Excluir informações críticas | A fonte da ameaça altera ou exclui dados essenciais para as operações comerciais diárias. |
| Crie certificados falsificados. | A fonte da ameaça compromete uma autoridade de certificação para fazer com que suas conexões pareçam legítimas. |
| Instale sniffers de rede persistentes e direcionados em sistemas de informações organizacionais. | A fonte da ameaça instala um software projetado para coletar (farejar) tráfego de rede durante um período de tempo contínuo. |
| Realizar ataques de negação de serviço (DoS). | A fonte da ameaça envia solicitações excessivas e automatizadas para sobrecarregar os recursos operacionais do sistema. |
| Interrompa operações de missão crítica. | A fonte da ameaça compromete a integridade das informações de tal forma que impede a empresa de realizar operações críticas. |
| Ofusque ataques futuros. | A fonte da ameaça toma medidas para inibir a eficácia dos sistemas de detecção de intrusão ou dos recursos de auditoria da empresa. |
| Realize ataques do tipo "man-in-the-middle". | A fonte de ameaça espiona sessões entre sistemas internos e externos. Mais tarde, eles retransmitem mensagens entre sistemas organizacionais e externos que os fazem acreditar que estão falando diretamente uns com os outros por uma conexão privada. |

## Probabilidade de um evento de ameaça

Em geral, a probabilidade de um evento de ameaça deve ser uma pontuação baseada em uma combinação de fatores. Por exemplo, qualquer evidência disponível que você tenha, experiência anterior e seu julgamento especializado.

Considere a intenção/capacidades de uma fonte de ameaça e eventos de ameaça em potencial ao produzir uma pontuação de probabilidade.

|  |  |  |
| --- | --- | --- |
| **Qualitative values** | **Quantitative values** | **Description** |
| High | 3 | A fonte da ameaça quase certamente iniciará um evento de segurança. Um evento pode ter efeitos múltiplos, severos ou catastróficos nas operações e ativos comerciais. |
| Moderate | 2 | A fonte da ameaça tem alguma probabilidade de iniciar um evento de segurança. Um evento pode reduzir significativamente a funcionalidade das operações e ativos organizacionais. |
| Low | 1 | É altamente improvável que a fonte da ameaça inicie um evento de segurança. Um evento pode ter efeitos menores e insignificantes nas operações e ativos comerciais. |

## Gravidade de um evento de ameaça

Em geral, a gravidade de um evento de ameaça é uma medida de seu impacto potencial nas operações comerciais. Por exemplo, o evento faria com que uma função comercial parasse completamente? Poderia interromper temporariamente um processo comercial e passar despercebido?

Considere o impacto comercial de eventos de ameaça ao produzir uma pontuação de gravidade.

|  |  |  |
| --- | --- | --- |
| **Qualitative values** | **Quantitative values** | **Description** |
| High | 3 | A fonte da ameaça quase certamente iniciará um evento de segurança. Um evento pode ter efeitos múltiplos, severos ou catastróficos nas operações e ativos comerciais. |
| Moderate | 2 | A fonte da ameaça tem alguma probabilidade de iniciar um evento de segurança. Um evento pode reduzir significativamente a funcionalidade das operações e ativos organizacionais. |
| Low | 1 | É altamente improvável que a fonte da ameaça inicie um evento de segurança. Um evento pode ter efeitos menores e insignificantes nas operações e ativos comerciais. |