# Categorias de controle

## Categorias de controle

Os controles dentro da segurança cibernética são agrupados em três categorias principais:

● Controles administrativos/gerenciais

● Controles técnicos

● Controles físicos/operacionais

Os controles administrativos/gerenciais abordam o componente humano da segurança cibernética. Esses controles incluem políticas e procedimentos que definem como uma organização gerencia dados e definem claramente as responsabilidades dos funcionários, incluindo seu papel na proteção da organização. Embora os controles administrativos sejam normalmente baseados em políticas, a aplicação dessas políticas pode exigir o uso de controles técnicos ou físicos.

Os controles técnicos consistem em soluções como firewalls, sistemas de detecção de intrusão (IDS), sistemas de prevenção de intrusão (IPS), produtos antivírus (AV), criptografia, etc. Os controles técnicos podem ser usados ​​de várias maneiras para atender às metas e objetivos organizacionais.

Os controles físicos/operacionais incluem fechaduras de portas, fechaduras de armários, câmeras de vigilância, leitores de crachás, etc. Eles são usados ​​para limitar o acesso físico a ativos físicos por pessoal não autorizado.

Tipos de controle

Os tipos de controle incluem, mas não estão limitados a:

1. Preventivo

2. Corretivo

3. Detetive

4. Dissuasor

Esses controles trabalham juntos para fornecer defesa em profundidade e proteger ativos. Os controles preventivos são projetados para evitar que um incidente ocorra em primeiro lugar. Os controles corretivos são usados ​​para restaurar um ativo após um incidente. Os controles de detecção são implementados para determinar se um incidente ocorreu ou está em andamento. Os controles de dissuasão são projetados para desencorajar ataques.

Revise os gráficos a seguir para obter detalhes específicos sobre cada tipo de controle e sua finalidade.

| **Administrative/Managerial Controls** | | |
| --- | --- | --- |
| **Nome do controle** | **Tipo de controle** | **Objetivo do controle** |
| Privilégio mínimo | Preventivo | Reduz o risco e o impacto geral de contas internas maliciosas ou comprometidas |
| Planos de recuperação de desastres | Corretivo | Fornecer continuidade de negócios |
| Políticas de senha | Preventivo | Reduza a probabilidade de comprometimento da conta por meio de técnicas de força bruta ou ataque de dicionário |
| Políticas de controle de acesso | Preventivo | Reforce a confidencialidade e a integridade definindo quais grupos podem acessar ou modificar dados |
| Políticas de gerenciamento de contas | Preventivo | Gerenciando o ciclo de vida da conta, reduzindo a superfície de ataque e limitando o impacto geral de ex-funcionários descontentes e uso de conta padrão |
| Separação de funções | Preventivo | Reduza o risco e o impacto geral de contas internas maliciosas ou comprometidas |

|  |  |  |
| --- | --- | --- |
| **Technical Controls** | | |
| **Control Name** | **Control Type** | **Control Purpose** |
| Firewall | Preventivo | Para filtrar tráfego indesejado ou malicioso para que não entre na rede |
| IDS/IPS | Detetive | Para detectar e prevenir tráfego anômalo que corresponda a uma assinatura ou regra |
| Criptografia | Dissuasor | Fornecer confidencialidade às informações sensíveis |
| Backups | Corretivo | Restaurar/recuperar de um evento |
| Gerenciamento de senhas | Preventivo | Reduza a fadiga de senha |
| Antivirus (AV) software | Corretivo | Detectar e colocar em quarentena ameaças conhecidas |
| Monitoramento, manutenção e intervenção manuais | Preventivo | Necessário para identificar e gerenciar ameaças, riscos ou vulnerabilidades em sistemas desatualizados |

|  |  |  |
| --- | --- | --- |
| **Physical/Operational Controls** | | |
| **Control Name** | **Control Type** | **Control Purpose** |
| Cofre com controle de tempo | Dissuasor | Reduza a superfície de ataque e o impacto geral de ameaças físicas |
| Iluminação adequada | Dissuasor | Deter ameaças limitando os locais de “esconderijo” |
| Closed-circuit television (CCTV) | Preventivo /Detetive | O circuito fechado de televisão é um controle preventivo e detetive porque sua presença pode reduzir o risco de certos tipos de eventos ocorrerem e pode ser usado após um evento para informar sobre as condições do evento |
| Armários de bloqueio (para equipamentos de rede) | Preventivo | Reforçar a integridade impedindo que pessoas não autorizadas e outros indivíduos acessem ou modifiquem fisicamente os equipamentos de infraestrutura de rede |
| Sinalização indicando prestador de serviço de alarme | Dissuasor | Deter certos tipos de ameaças, fazendo com que a probabilidade de um ataque bem-sucedido pareça baixa |
| Fechaduras | Dissuasor/Preventivo | Reforçar a integridade, dissuadindo e impedindo que pessoas e indivíduos não autorizados se aproximem fisicamente accessing assets |
| Detecção e prevenção de incêndio (alarme de incêndio, sistema de sprinklers, etc.) | Detetive / Preventivo | Detecte incêndios em locais físicos e evite danos a ativos físicos, como estoque, servidores, etc. |