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

Controles administrativos/gerenciais: abordar o componente humano da segurança cibernética. Esses controles incluem políticas e procedimentos que definem como uma organização gerencia dados e define 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.

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 diversas maneiras para atender às metas e objetivos organizacionais.

Controles físicos/operacionais incluem fechaduras de portas, fechaduras de armários, câmeras de vigilância, leitores de crachás, etc. Elas são usadas 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. Dissuasivo

Esses controles trabalham juntos para fornecer defesa em profundidade e proteger ativos.**Controles preventivos** são projetados para evitar que um incidente ocorra em primeiro lugar.**Controles corretivos** são usados para restaurar um ativo após um incidente.**Controles de detetive** são implementadas para determinar se um incidente ocorreu ou está em andamento.**Controles dissuasivos** são projetados para desencorajar ataques.

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

Administrativo/Gerencial Controles		
Nome do controle	**Tipo de controle**	**Controle Propósito**
Mínimo Privilégio	Preventivo	Reduzir o risco e 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 impacto geral de ex-funcionários descontentes e uso de conta padrão

Administrativo/Gerencial Controles		
Separação de funções	Preventivo	Reduzir o risco e impacto geral de contas internas maliciosas ou comprometidas

Controles Técnicos		
Nome do controle	**Tipo de controle**	**Finalidade do controle**
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	Dissuasivo	Fornecer confidencialidade às informações sensíveis
Backups	Corretivo	Restaurar/recuperar de um evento
Gerenciamento de senhas	Preventivo	Reduza a fadiga de senhas
Software antivírus (AV)	Preventivo	Verificações para 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

Controles Físicos/Operacionais		
Nome do controle	**Tipo de controle**	**Finalidade do controle**
Cofre com controle de tempo	Dissuasivo	Reduza a superfície de ataque e impacto geral de ameaças físicas
Iluminação adequada	Dissuasivo	Deter ameaças limitando os locais de “esconderijo”
Circuito fechado de televisão (CFTV)	Preventivo/Detetive	O circuito fechado de televisão é um controle preventivo e detetive porque sua presença pode reduzir o risco de ocorrência de certos tipos de eventos e pode ser usado após um evento para informar sobre as condições do evento.
Armários com trava (para equipamentos de rede)	Preventivo	Reforçar a integridade impedindo que pessoas não autorizadas e outros indivíduos acessem ou modifiquem fisicamente os equipamentos da infraestrutura de rede
Sinalização indicando prestador de serviço de alarme	Dissuasivo	Deter certos tipos de ameaças, fazendo com que a probabilidade de um ataque bem-sucedido pareça baixa
Fechaduras	Dissuasor/Preventivo	Reforçar a integridade, impedindo e impedindo que pessoas e indivíduos não autorizados acessem fisicamente os ativos
Detecção e prevenção de	Detetive/Preventivo	Detecte incêndios em

incêndio (alarme de incêndio, sistema de sprinklers, etc.)		locais físicos e evite danos a ativos físicos, como estoque, servidores, etc.