POLÍTICA DE ANTIVÍRUS

Autores: André Marques, Bruno Correa Fausto

Data de Criação: 06/02/2024

Última Atualização: 06/02/2024

Versão: 1ª

O objetivo de uma política de antivírus gerenciado em uma empresa é garantir a segurança da rede, dos sistemas e dos dados contra ameaças cibernéticas, como vírus, malware, spyware e outras formas de software malicioso. Aqui estão alguns dos principais objetivos:

1. Proteção contra Ameaças Cibernéticas:

- Garantir que todos os dispositivos na rede estejam protegidos contra vírus e malware.

- Detectar e bloquear ameaças em tempo real para evitar danos aos sistemas e dados.

2. Atualizações Automáticas:

- Assegurar que as definições de vírus e as atualizações do software antivírus sejam aplicadas automaticamente em todos os dispositivos conectados à rede.

3. Conformidade e Políticas de Segurança:

- Garantir que a empresa esteja em conformidade com regulamentações de segurança e políticas internas relacionadas à proteção contra ameaças cibernéticas.

4. Monitoramento e Relatórios:

- Monitorar continuamente a atividade de antivírus para identificar possíveis ameaças.

- Gerar relatórios para avaliar a eficácia das medidas de segurança e tomar ações corretivas, se necessário.

5. Controle Centralizado:

- Gerenciar todas as soluções antivírus de forma centralizada, facilitando a implementação de políticas de segurança consistentes em toda a organização.

6. Minimização de Riscos:

- Reduzir o risco de infecção por malware, que pode levar a perda de dados, interrupção de operações e danos à reputação da empresa.

7. Proteção de Dados Sensíveis:

- Proteger dados sensíveis da empresa contra acesso não autorizado e roubo por meio de ataques cibernéticos.

8. Eficiência Operacional:

- Manter a eficiência operacional, evitando interrupções causadas por infecções de malware.

9. Resposta a Incidentes:

- Estabelecer procedimentos para lidar com incidentes de segurança, como isolamento de sistemas comprometidos e recuperação de dados.

10. Conscientização dos Usuários:

- Educar os usuários sobre práticas seguras na internet, alertando sobre possíveis ameaças e promovendo uma cultura de segurança cibernética na organização.

Ao implementar uma política de antivírus gerenciado, a empresa pode fortalecer suas defesas cibernéticas e reduzir significativamente os riscos associados a ameaças online.

Segue abaixo aos parâmetros empregados ao antivírus gerenciado:

- Excluir itens que estejam na quarentena a mais de 30 dias;
- Definições de ameaças são atualizadas a cada 6 horas;
- Verificações rápidas:
    - Está verificação visa verificar locais comuns de ameaça, sendo uma pouco mais rápida que verificação profunda, é executada de segunda-feira a quinta-feira 12:15Hrs;
- Verificação profunda:
    - Está verificação visa verificar todas as unidades fixas e removíveis do computador (HDs, SSDs, pendrives, HDs Externos etc.), é executada toda sexta-feira 12:15Hrs;

Possui também exclusões em sua configuração, exclusões seriam os arquivos, pastas ou extensões que devam ser excluídos da verificação do antivírus, como por exemplo os arquivos da pasta SCI, que podem ser confundidos como falso positivo, e comprometer a produtividade da empresa.