Mantendo a segurança

Mantenha a segurança no seu ambiente do Archer seguindo práticas recomendadas do setor.

Nesta página

Gerenciamento de patch de segurança

Os patches de segurança são lançados conforme necessário.

Todos os patches de segurança do Archer estão disponíveis para download como uma atualização de clientes com um acordo de manutenção atual do Archer. Há atualizações disponíveis em Archer Community.

Execute os patches de segurança mais recentes para qualquer software que você esteja usando com o Archer e certifique-se de usar o software compatível mais recente. Consulte Ambientes qualificados e compatíveis do Archer para obter o software e os ambientes, navegadores e ferramentas qualificados e compatíveis.

Aqui está uma lista de componentes de terceiros para os quais os patches são necessários. A frequência das atualizações do patch é determinada pelo fornecedor. É responsabilidade do cliente garantir que os componentes de terceiros sejam corrigidos conforme apropriado, usando as instruções fornecidas pelo fornecedor.

- Windows Server
- SQL Server
- Microsoft IIS

- .NET Framework

Detecção de malware

Implemente uma solução de detecção de malware nos servidores da Web e de banco de dados. A solução de detecção de malware deve ser baseada em suas ferramentas padrão e práticas recomendadas. É de sua responsabilidade a implementação de patches e atualizações para as ferramentas de detecção de malware.

Varredura de vírus

Execute um software de varredura de vírus nos servidores implementados de modo rotineiro. Se você estiver executando Alimentadores de ameaça ou de vulnerabilidade, é altamente recomendável que você desative a verificação de vírus na pasta em que os arquivos de dados de ameaça ou de vulnerabilidade estão temporariamente armazenados. O mecanismo de verificação de vírus pode interpretar os dados como um vírus ou malware.

Monitoramento e auditoria contínuos

Como com qualquer componente essencial de infraestrutura, monitore constantemente o sistema e realize auditorias periódicas e aleatórias. Assegure-se de que as configurações e definições de acesso do usuário sejam compatíveis com as políticas e necessidades de sua empresa.

Proteção das credenciais

A seleção do algoritmo de hash para credenciais usa o algoritmo PBKDF2 com um tamanho de salt gerado aleatoriamente.