Instalação de softwares de terceiros no senhasegura

senhasegura

Departamento de Segurança e Inovação - SEGi9

1 de junho de 2023

CONFIDENCIAL

Sumário

1 Objetivo

Segurança e Confiabilidade são dois itens importantes em um sistema de segurança crítico de uma empresa. Esse texto tem por objetivo o de demonstrar o por que esses dois itens são tão importantes para a empresa MT4, desenvolvedora da aplicação PAM senhasegura.

2 Segurança e Confiabilidade

Em um ambiente de missão crítica como o senhasegura, onde são armazenados uma série de informações privilegiadas, as caracteristicas segurança e confiabilidade são prioritárias. O time engenharia do senhasegura executam uma série de hardenings para garantir a segurança e confiabilidade da aplicação.

Nas sessões subsequentes serão detalhados as atividades realizadas pela empresa MT4 para garantir a segurança e confiabilidade do senhasegura.

2.1 Auditoria

De forma periódica, a empresa MT4 contrata empresas lideres de mercado da área de segurança para realizarem um processo de auditoria sobre a aplicação senhasegura e sobre o sistema operacional que a hospeda, chamado pentest. O objetivo desta auditoria é o de procurar possíveis falhas de seguranças e melhorias que possam ser realizadas. A partir de um relatório final fornecido pela empresa contratada, são aplicadas as recomendações na aplicação, cujo objetivo é o de torna-la ainda mais segura.

2.2 Hardening

O sistema operacional onde o senhasegura é hospedado sofre um processo de hardening, onde é feito uma análise minuciosa e constante do sistema operacional em busca de serviços, configurações padrão e portas lógicas desnecessárias que são desabilitadas, para que a aplicação possa funcionar de forma correta e segura.

2.3 Wazuh

A solução de segurança Wazuh, do tipo EDR (Endpoint Detection and Response) tem por objetivo o de detectar ameaças, tentativas de intrusão, ações

de usuários não autorizados e fornecer análises de segurança. Com essas informações coletadas e analisadas, a ferramenta Wazuh cria uma série de respostas automatizadas para combater um possível ataque.

2.4 Firewall

A senhasegura possui um firewall interno que monitora de forma constante as tentativas de logon na aplicação com objetivo de detectar possíveis tentativas de ataque. A partir do momento em que a tentativa de acesso é classificada como um ataque, os endereços IPs de origem da ação são bloqueados de forma automática.

2.5 Confiabilidade

Confiabilidade de software é definida em termos gerais como a "probabilidade de operação livre de falhas de um programa de computador, em um ambiente especificado, durante um tempo especificado". Quando um software de terceiro é instalado junto a uma aplicação, isso pode causar uma instabilidade.

Um exemplo de instabilidade gerada por um software de terceiro, ocorre quando o software instalado tem por objetivo o de monitorar o trafego de acesso ao servidor de banco de dados SQL, para evitar um ataque do tipo SQL Injection, mas acaba causando uma lentidão ou instabilidade na operação.

2.6 Monitoramento

A senhasegura possui uma série de ferramentas e protocolos disponíveis para o administrador e que são utilizados para o monitoramento e manutenção da aplicação. Segue abaixo uma lista dos itens disponíveis.

- agente Zabbix, que pode ser integrado ao servidor Zabbix;
- protocolo SNMP utilizado para o fornecimento de informações sobre a saúde da aplicação;
- integração nativa para aplicações do tipo SIEM.

2.7 Supply Chain

Com a finalidade de evitar ataques do tipo supply chain, o senhasegura proibe a instalação de softwares de terceiros na aplicação.
Um exemplo de ataque do tipo Supply Chain, foi o caso SolarWinds, onde um grupo de cibercriminosos obteve acesso ao ambiente empresarial por meio de uma atualização comprometida do software Orion. Após a invasão, o hacker usou esse acesso para produzir e distribuir atualizações carregadas de trojan aos usuários do software, espalhando-se por redes altamente estratégicas. Bastou a instalação de um software para comprometer toda a segurança da rede corporativa.

3 Conclusão

No começo deste documento, foram mencionados os atributos Segurança e Confiabilidade. Dado que a aplicação PAM senhasegura lida com informações altamente sensíveis, como credenciais de acesso a servidores e estações de trabalho presentes na rede empresarial, a equipe de segurança da MT4 adota uma abordagem focada na eficiência. Minimizar a quantidade de componentes no ambiente em que a aplicação PAM senhasegura está instalada resulta em um nível de segurança mais robusto.

4 Termos e condições

No item "Uso de Software"dos Termos e condições da MT4, descrito abaixo, especifica a proibição da instalação de qualquer software de terceiros na aplicação senhasegura.

Ao instalar e utilizar nosso software, você concorda com os seguintes termos e condições:

- **Não é permitido instalar software de terceiros dentro do sistema operacional do nosso produto;**
- **A instalação de qualquer software de terceiros sem autorização da empresa senhasegura pode interferir no desempenho e estabilidade do nosso produto, causar mal funcionamento do produto e não é permitido.**

Para mais informações, basta consultar as seguintes URLs:

- senhasegura EULA
- Termos e condições

Controle do Documento
FSR-1052

Contato
Suporte support@senhasegura.com