AÇÕES DE REMEDIAÇÃO SEGUINTES O INCIDENTE DO SENSOR CHIYU IMPLANTADO PELA SOLAR-OT

Implantação da última versão de firmware e Hardening da plataforma Supervisão SOLAR-OT

Autor	Validado por
Deirdre STARSKY, Gerente de Projeto Técnico	Elena PIZARI, Diretora Geral Indústria

OBJETIVO

Este documento especifica as 2 ações de remediação após o incidente nos sistemas de controle de acesso implantados pela SOLAR-OT:

1. Implantação emergencial de atualização de firmware em todos os sistemas
2. Reforçar a configuração da plataforma de supervisão

1. IMPLEMENTAÇÃO DE EMERGÊNCIA DA ATUALIZAÇÃO DE FIRMWARE

O fabricante CHIYU desenvolveu uma atualização de firmware para os sistemas de controle de acesso 'SEMAC' corrigindo a vulnerabilidade => deve ser implantada pela SOLAR-OT com urgência em todos os sites

Aqui está o número da versão do firmware a ser implantada no SEMAC S2 (67% da frota): 670VYJLN
Aqui está o número da versão do firmware a ser implantada no SEMAC S3V3 (33% da frota): 628AUYSD

2. FORTALECENDO A CONFIGURAÇÃO DA PLATAFORMA SUPERVISÃO

CONFIGURAÇÃO

O objetivo é limitar os elementos técnicos que podem ser utilizados para realizar um ataque, instalando apenas serviços e equipamentos essenciais.

O reforço do nível de segurança requer reforço, incluindo:

- Limitação das funções da plataforma
- Domínio dos elementos de hardware da plataforma

A. Modificação da configuração padrão

Cada componente é configurado de acordo com padrões, incluindo:

- Contas técnicas e elementos de autenticação associados
- Portas de rede usadas
- Diretórios de instalação e trabalho
- Direitos de acesso a diretórios e arquivos
- A conta usada para executar um serviço ou processo e os direitos associados a esta conta
- Arquivos de configuração de elementos de segurança, em particular rastreabilidade.

B. Restrição de funcionalidades acessíveis

Apenas os módulos essenciais ao funcionamento e segurança da plataforma são mantidos e são sujeitos a configuração adequada, manutenção regular e supervisão.

Como tal, o operador analisa o funcionamento técnico da plataforma para excluir serviços ou funcionalidades instaladas mas não utilizadas.

Cada configuração de hardware ou software é inventariada na forma de uma configuração de referência.

C. Inventário de elementos conectados

O operador realiza um inventário técnico completo dos elementos que constituem a plataforma e os mapeia. O inventário inclui equipamentos que podem se conectar à plataforma de forma permanente ou temporária, física ou remota (estação de trabalho, servidor, periférico, etc.).

Caso um terceiro se conecte à plataforma, a operadora anota isso em seu mapeamento e leva em consideração na análise de risco.

D. Uso de elementos controlados

O operador gerencia os elementos diretamente, incluindo:

- Implantação de atualizações
- Administração de elementos
- Configuração remota

PARTICIONAMENTO

A plataforma segue uma lógica de segmentação restringindo cada subsistema às suas próprias ações de forma a:

- Limitar a superfície de ataque
- Conter um possível ataque
- Limitar o impacto de um compromisso
- Permitir que o nível de segurança de cada subsistema seja adaptado

A compartimentalização se aplica a meios físicos e lógicos.

A. Segmentação em subsistemas

A segmentação em subsistemas é realizada de acordo com os seguintes critérios:

- Características
- Nível de proteção de dados
- Nível de exposição
- Nível de segurança

Qualquer ligação entre subsistemas deve ser justificada por uma necessidade funcional.

B. Particionamento físico

Um servidor é dedicado às aplicações mais críticas

C. Particionamento lógico

Todos os dados armazenados no servidor são criptografados previamente. Cada subsistema segue seu próprio mecanismo de criptografia.

Toda a comunicação entre os subsistemas passa pela rede privada virtual criptografada e autenticada.

ACESSO REMOTO

A. Acesso público

O acesso público segue o protocolo HTTPS e a plataforma é autenticada pela apresentação de um certificado servidor.

A autenticação de dois fatores é implementada para usuários da plataforma.

B. Acesso nômade

As estações de trabalho nômades são configuradas para estabelecer o túnel autenticado e criptografado para a plataforma.
O túnel não pode ser desativado e o acesso à Internet ou a uma rede local é impossível.
A partição do sistema e a partição de dados são totalmente criptografadas

A autenticação de dois fatores está em vigor na estação de trabalho.

FILTRAGEM DE REDE

Além da compartimentação, são implementados mecanismos de filtragem.

A. Pontos de filtro

As interligações entre subsistemas são os principais pontos de filtragem aos quais são aplicadas a filtragem perimetral e local.

B. Regras de filtragem

A matriz de fluxo geral inclui as regras de filtragem em vigor. Ele é atualizado anualmente.

C. Implementação

A filtragem é assegurada por firewalls dedicados baseados no princípio das listas de autorização.