AÇÕES DE REMÉDIATION SUITE À O INCIDENTE COM OS CAPITÃES CHIYU IMPLANTADOS PELA SOLAR-OT

Implementação da última versão dos firmwares e encerramento da plataforma de supervisão SOLAR-OT

Autor	Validado pelo senhor
Deirdre STARSKY, Chefe de projeto técnico	Elena PIZARI, Diretora Geral da Indústria

OBJETIVO

O presente documento resume as duas ações de remediação decorrentes do incidente com os sistemas de controle de acesso implantados pela SOLAR-OT:

1. O uso em caráter de urgência do micrologiciel em todos os sistemas
2. O reforço da configuração da plataforma de supervisão

1. IMPLEMENTAÇÃO EM CARÁTER DE URGÊNCIA DO MICROLOGICIEL

O construtor CHIYU desenvolveu um modelo do micrologiciel dos sistemas "SEMAC" de controle de acesso que corrige a vulnerabilidade => ele deve ser implantado pela SOLAR-OT com urgência em todos os locais

Veja o número da versão do micrologiciel a ser implantada no SEMAC S2 (67% do lote): 670VYJLN Veja o número da versão do micrologiciel a ser implantada no SEMAC S3V3 (33% do lote): 628AUYSD

2. REFORÇO DA CONFIGURAÇÃO DA PLATAFORMA DE SUPERVISÃO

CONFIGURAÇÃO

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

O reforço do nível de segurança passa por um processo que inclui :

- A limitação das funções da plataforma
- O domínio dos elementos materiais da plataforma

A. Modificação da configuração por falha

Cada componente é configurado de acordo com os padrões, incluindo :

- As contas técnicas e os elementos de autenticação associados
- As portas são utilizadas
- Os relatórios de instalação e de trabalho
- Os direitos de acesso aos relatórios e arquivos
- O computador utilizado para executar um serviço ou um processo, e os direitos associados a esse computador
- Os arquivos de configuração dos elementos de segurança, em particular os de traçabilidade.

B. Restrição de funcionalidades acessíveis

Somente os módulos indispensáveis ao funcionamento e à segurança da plataforma são mantidos e são objeto de uma configuração adequada, de uma manutenção regular e de uma supervisão.

A esse título, o operador analisa o funcionamento técnico da plataforma para excluir os serviços ou funcionalidades instaladas, mas não utilizadas.

Cada configuração material ou lógica é inventada sob a forma d e uma configuração de referência.

C. Inventário de elementos conectados

O operador utiliza um inventário técnico completo dos elementos que compõem a plataforma e a cartografia. O inventor inclui os equipamentos que podem se conectar à plataforma de forma permanente ou temporária, física ou à distância (posto de trabalho, servidor, periférico...).

No caso de uma terceira parte se conectar à plataforma, o operador deve anotar em sua cartografia e em O senhor deve levar em conta na análise de riscos.

D. Utilização de elementos aprendidos

O operador recebe os elementos diretamente, como :

- O uso de ferramentas de trabalho
- A administração dos elementos
- A configuração à distância

CLOISONNEMENT

A plataforma segue uma lógica de segmentação, restabelecendo cada sistema único p a r a suas próprias ações, com o objetivo de :

- Limitar a superfície de ataque
- Contém um ataque eventual
- Limitar o impacto de um compromisso
- Permitir a adaptação do nível de segurança de cada sistema

O cloisonnement se aplica tanto a meios físicos quanto a meios logísticos.

A. Segmentação em sistemas de sensores

A segmentação em sistemas de pesquisa é feita de acordo com os seguintes critérios:

- Funcionalidades
- Nível de proteção dos dados
- Nível de exposição
- Nível de segurança

Toda conexão entre os sistemas de dados deve ser justificada por uma necessidade funcional.

B. Cloisonnement physique

Um servidor é dedicado aos aplicativos mais críticos

C. Cloisonnement logique

Todos os dados armazenados no servidor são codificados no pré-sal. Cada sistema secundário tem um mecanismo de controle próprio.

Toda a comunicação entre os sistemas sous é feita por meio da rede privada virtual, verificada e autenticada.

ACESSA A DISTÂNCIA

A. Acesso público

O acesso público é feito pelo protocolo HTTPS e a plataforma é autenticada pela apresentação de um certificado Servir.

A autenticação de duplo fator foi implementada para os usuários da plataforma.

B. Acesso nômade

Os postes nômades são configurados para estabelecer o túnel autenticado e compartilhado com a plataforma. O túnel
não pode ser desativado, e o acesso à Internet ou a uma rede local é impossível.
O sistema de partição e a partição de dados são integralmente compartilhados

A autenticação com duplo fator está em vigor no posto de trabalho.

FILTRAGEM DE RESÍDUOS

Em complemento ao cloisonnement, são utilizados mecanismos de filtragem.

A. Pontos de filtragem

As interconexões entre os sistemas de sous são os principais pontos de filtragem aos quais são aplicados os filtros periféricos e locais.

B. Regras de filtragem

A matriz de fluxo global inclui as regras de filtragem em vigor. Ela é atualizada anualmente.

C. Execução

A filtragem é assegurada por um parente dedicado que se baseia no princípio das listas de autorização.