CHECKLIST TÉCNICO

Segurança de Dados em Ambientes OT/IT Convergidos

Um guia prático para times de TI industrial e CISOs avaliarem riscos e priorizarem ações na convergência entre Tecnologia Operacional e Tecnologia da Informação.

Aplicável a todos os segmentos industriais

www.sdbit.com.br

SDB

Use este checklist para mapear rapidamente os principais pontos de atenção em segurança na convergência OT/IT da sua operação. Marque os itens já implementados e priorize os pendentes com sua equipe de TI e OT.

1. Visibilidade e Inventário de Ativos

- Existe um inventário atualizado de todos os ativos (CLPs, IHMs, RTUs, *gateways* IIoT)?
- As versões de *firmware* e *software* desses ativos são documentadas e monitoradas?
- Há visibilidade em tempo real do tráfego de rede entre zonas OT e IT?
- Ativos legados sem suporte do fabricante foram identificados e mapeados como risco?

2. Segmentação e Arquitetura de Rede

- A rede está segmentada em zonas e conduítes, conforme a norma IEC 62443?
- Existe uma DMZ industrial entre as redes corporativa (IT) e de controle (OT)?
- As comunicações entre zonas passam por *firewalls* ou *gateways* com inspeção de protocolo?
- A microssegmentação é aplicada a ativos críticos dentro da própria rede OT?

3. Controle de Acesso e Identidade

- O acesso remoto de fornecedores e integradores exige autenticação multifator?
- As sessões remotas de terceiros são monitoradas e registradas em log?
- Existe política de privilégio mínimo aplicada a usuários e sistemas em ambiente OT?
- Os princípios de *Zero Trust* foram adaptados às restrições operacionais da planta?

4. Monitoramento e Detecção

- Há solução de IDS/IPS específica para protocolos industriais (*Modbus*, OPC-UA etc.)?
- Existe um processo definido de resposta a alertas de segurança em ambiente OT?
- O SOC (interno ou terceirizado) tem visibilidade e conhecimento técnico sobre OT?

5. Gestão de *Patches* e Vulnerabilidades

- Existe processo formal de avaliação de vulnerabilidades em ativos OT?
- As atualizações críticas são aplicadas dentro de janelas de manutenção planejadas?
- Há controles compensatórios definidos para ativos que não podem ser atualizados?

6. Governança, Cultura e Resposta a Incidentes

- Existe um comitê ou fórum conjunto entre lideranças de TI e OT?
- Times de TI e OT compartilham métricas e prioridades de segurança comuns?
- Há um plano de resposta a incidentes específico para cenários OT?
- As equipes de operação recebem treinamento periódico sobre riscos cibernéticos?
- A empresa utiliza *frameworks* de referência (IEC 62443, NIST CSF, ISA-95) para orientar sua
- estratégia?

Como usar este checklist

Priorize os itens não marcados nas seções 1 e 2 já que o inventário e a segmentação são a base de qualquer estratégia de segurança OT/IT.

Em seguida, avance para controle de acesso, monitoramento e governança.

Se você quer acabar com as falhas que identificou
mas não sabe por onde começar, nós podemos te ajudar.
Entre em contato agora mesmo!

SDB

www.sdbit.com.br