H-CYBER ICS

(SERVIÇO DE CIBERSEGURANÇA NO ÂMBITO DE SISTEMAS DE CONTROLO INDUSTRIAIS (ICS))

CYBER EFFECT - NÍVEL 1 - REATIVO

DESCRIÇÃO

O Serviço de Cibersegurança no âmbito de Sistemas de Controlo Industriais, fornece mecanismos, processos e técnicas sobre como proteger Sistemas de Controlo Industrial, incluindo sistemas de Controlo de Supervisão e Aquisição de Dados (SCADA), Sistemas de Controlo Distribuído (DCS), e outras configurações de sistemas de controlo, tais como Controladores Lógicos Programáveis (PLC), de forma a garantir o seu desempenho, fiabilidade e requisitos de segurança. Os nossos serviços fornecem uma visão geral da segurança para ICS, bem como topologias típicas de sistemas, identificando ameaças e vulnerabilidades orientados a estes sistemas, fornecendo e recomendando contramedidas de segurança para mitigar os riscos associados.

PROPOSTA DE VALOR

Os ICS tem muitas características, que diferem dos sistemas TI tradicionais, incluindo diferentes riscos e prioridades de negócio. Alguns incluem riscos significativos para a saúde e segurança de vidas humanas, danos graves para o ambiente e questões financeiras tais como perda de produção e impacto negativo para as empresas/governo. Criamos e fornecemos soluções que garantem a proteção adequada, de forma a manter a integridade do sistema durante as operações normais, bem como durante períodos de ciberataques, em conformidade com as normas IEC 62443, NERC e NIST.

Seguem algumas das áreas operacionais de negócio cobertas pelas nossas soluções de Cibersegurança no âmbito do ICS:

- Holdings, aeroespacial, naval, terrestre.
- Robótica e automação.
- Defesa.

Rua Acácio de Paiva 16
1ºD - 1700-006 Lisboa
www.hardsecure.com
(+351) 218 278 126
geral@hardsecure.com

H-CYBER ICS

(SERVIÇO DE CIBERSEGURANÇA NO ÂMBITO DE SISTEMAS DE CONTROLO INDUSTRIAIS (ICS))

CYBER EFFECT - NÍVEL 1 - REATIVO

- Industria têxtil.
- Energia e Transporte.
- Ambiente e segurança.
- Sistemas de Sinalização Digital.
- Sistemas de Segurança Eletrónica.
- Sistemas de Gestão de Emergência.
- Sistemas de Controlo de Instrumentos de Laboratório & Healthcare.
- Sistemas de Gestão de Informação de Laboratório (LIMS).

CARACTERÍSTICAS DO SERVIÇO

A implementação do ICS inclui as seguintes características:

Restrição do acesso lógico à rede ICS e à atividade da rede. Isto pode incluir a utilização de gateways unidirecionais (díodos), arquitetura de rede de zona desmilitarizada (DMZ) com firewalls para impedir que o tráfego de rede passe diretamente entre as redes corporativas e os ICS, fornecer mecanismos e credenciais de autenticação separados para os utilizadores das redes corporativas e redes de ICS.

Restrição do acesso físico à rede e dispositivos ICS. O acesso físico não autorizado aos componentes poderá causar graves perturbações na funcionalidade do ICS. Deve ser utilizada uma combinação de controlos de acesso físico, tais como fechaduras, leitores de cartões, e/ou guardas.

Restringir a modificação não autorizada de dados. Isto inclui dados que estão em trânsito (pelo menos através dos limites da rede) e armazenados em endpoints/shares de rede.

Rua Acácio de Paiva 16
1ºD - 1700-006 Lisboa
www.hardsecure.com
(+351) 218 278 126
geral@hardsecure.com

H-CYBER ICS

(SERVIÇO DE CIBERSEGURANÇA NO ÂMBITO DE SISTEMAS DE CONTROLO INDUSTRIAIS (ICS))

CYBER EFFECT - NÍVEL 1 - REATIVO

➤ **Proteger os componentes individuais do ICS contra ataques informáticos.** Isto inclui a implementação de patches de segurança da forma mais rápida, depois de os testar em ambiente de qualidade; Desativar todas as portas e serviços não utilizados e assegurar que permanecem desativados; Restringir os privilégios dos utilizadores do ICS apenas aos que são necessários para a função de cada colaborador; Rastrear e monitorizar tracks de auditoria; Utilizar controlos de segurança tais como software antivírus e software de verificação de integridade de ficheiros, sempre que tecnicamente seja possível, para prevenir, deter, detetar e mitigar malware.

➤ **Deteção de eventos e incidentes de segurança.** A deteção de eventos de segurança, que ainda não se converteram em incidentes, pode ajudar a organização a quebrar a cadeia de ataque antes dos atacantes atingirem os seus objetivos. Isto inclui a capacidade de detetar ataques falhados a componentes ICS, serviços indisponíveis, e recursos overloaded, que são importantes para proporcionar um funcionamento adequado e seguro dos ICS.

➤ **Manutenção da funcionalidade durante condições adversas.** Isto implica conceber o ICS de modo a que cada componente crítico tenha uma capacidade redundante. Além disso, se um componente falhar, deve falhar de forma a não gerar tráfego desnecessário na rede, ou a não causar outro problema num local diferente, tal como um evento em cascata.

➤ **Restauro do sistema após um incidente.** Os incidentes são inevitáveis e um plano de resposta a incidente é essencial. Uma característica principal de um bom programa de segurança é a rapidez com que o sistema pode ser recuperado após a ocorrência de um incidente.

➤ **Serviços operacionais de Cibersegurança.** Realizamos as seguintes atividades:

- Segregação e segmentação.
- Gestão do controlo de acesso dos utilizadores.
- Atualização e gestão de atualizações.
- Execução de verificações de validação.
- Aumento da segurança física.
- Criamos Planos de Resposta a Incidentes.
- Formação de colaboradores sobre como identificar ataques, como proteger a sua informação pessoalmente identificável, e como se proteger contra ataques.
- Mantemos um registo atualizado dos ativos da organização.

Rua Acácio de Paiva 16
1ºD - 1700-006 Lisboa
www.hardsecure.com
(+351) 218 278 126
geral@hardsecure.com

H-CYBER ICS

(SERVIÇO DE CIBERSEGURANÇA NO ÂMBITO DE SISTEMAS DE CONTROLO INDUSTRIAIS (ICS))

CYBER EFFECT - NÍVEL 1 - REATIVO

VALOR ACRESCENTADO

Iniciar uma iniciativa de cibersegurança para sistemas industriais não é uma tarefa tão assustadora ou um investimento tão grande como poderá parecer. Os danos substanciais que um ataque informático pode provocar, conduz as organizações a repensar as suas prioridades no âmbito do ICS.

Nós implementamos a cibersegurança em ICS através da operacionalização de cinco fases, nomeadamente:

Fase 1: Conceção e enquadramento

A conceção de um sistema de gestão de cibersegurança é a fase mais abrangente e requer o maior investimento em tempo e esforço, tanto do lado da Hardsecure, como do lado da organização. Nesta tarefa, incluímos a identificação de todos os ativos, sistemas e pessoas, a definição das suas funções, a definição dos seus direitos de controlo e acesso, e políticas existentes (ou necessárias) em torno destes parâmetros de forma a garantir operações seguras e robustas.

Fase 2: Avaliação de vulnerabilidades

A nossa fase de avaliação consiste principalmente em rever a conceção da cibersegurança, e identificar potenciais vulnerabilidades e riscos dependendo do impacto sobre o negócio/organização. As vulnerabilidades identificadas são atualizadas/corrigidas periodicamente. As avaliações são realizadas, utilizando a nossa equipa de Análise de Vulnerabilidades e Testes de Intrusão e várias ferramentas que coletam pacotes de dados ao nível da rede e identificam comportamentos anómalos e falhas do sistema.

Fase 3: Implementação

Esta parte é onde implementamos políticas, procedimentos e serviços técnicos, bem como boas práticas de cibersegurança, assegurando que todos os controlos dos standards e frameworks (de acordo com o negócio) são validadas. Um método chave de implementação é a implementação de zero-trust ao sistema/ativos críticos do negócio.

Fase 4: Auditoria

A auditoria de segurança abrange tarefas como testes abrangentes de intrusão (web, infraestrutura, mobile, aplicacional, bases de dados,...) para assegurar que a implementação está a atingir os resultados pretendidos. As nossas equipas especializadas em Pentest & auditoria, orientam este

H-CYBER ICS

(SERVIÇO DE CIBERSEGURANÇA NO ÂMBITO DE SISTEMAS DE CONTROLO INDUSTRIAIS (ICS))

CYBER EFFECT - NÍVEL 1 - REATIVO

trabalho e apoiam na garantia de uma sólida cibersegurança na organização. Contudo, podemos dar formação à equipa interna de auditoria da organização, para executar todas estas fases.

» Fase 5: Suporte e Manutenção
Para garantir um determinado nível de conformidade, será necessário assegurar a manutenção e o apoio do esforço que foi inicialmente realizado. Criamos valor na garantia da gestão, controlo e monitorização das infraestruturas, a fim de manter compliance nos controlos em toda a infraestrutura (dentro do âmbito).

PEDIDOS DE PROPOSTA / INFORMAÇÃO

Para informações adicionais ou mais esclarecimentos, por favor entre em contato através de um dos seguintes meios:

Formulário "Hardsecure – Serviço de Cibersegurança no Âmbito de Sistemas de Controlo Industriais (ICS)" (disponibilizado na página do serviço no website)

Comercial da Hardsecure:
(+351) 218 278 126
geral@hardsecure.com

Website:
www.hardsecure.com (Formulário **"Solicitar Proposta"**)