CYBERSEGURANÇA EM SISTEMAS DE GESTÃO TÉCNICA

A importância da certificação ISA 62443

TODOS OS SISTEMAS LIGADOS À REDE PODEM ENFRENTAR AMEAÇAS INFORMÁTICAS

As ameaças informáticas continuam a desenvolver-se e a escalar, e não há quaisquer evidências que mostrem que esta tendência vá abrandar nos próximos anos. Já não são apenas os computadores ou as redes informáticas que estão em risco. As tecnologias operacionais (OT) e as redes OT, tais como a Gestão Técnica de Edifícios, estão cada vez mais em risco – em parte porque podem ser uma porta de acesso à totalidade da rede informática de uma organização.

Por vezes, pode parecer que nenhuns sistemas ou dados estão a salvo de eventuais ataques – seja por parte de miúdos a brincar com programação, que só querem mostrar o que conseguem fazer ou maus atores em busca de extorquir dinheiro.

Os atacantes de nível governamental podem ser particularmente insidiosos e ter múltiplos objetivos: roubar propriedade intelectual para beneficiar a sua própria economia; interferir com infraestruturas sensíveis como o setor da energia; ou alcançar outros objetivos políticos e militares causando interferências.

Desde telemóveis até à automação de edifícios, todos dependemos dos produtos digitais e dos sistemas conectados, que usamos e damos como garantidos, mas como podemos ter a certeza que eles são resistentes a ataques informáticos?

Por exemplo, como é que os engenheiros de sistemas e integradores sabem quais os produtos que estão mais bem protegidos quando estão a projetar um novo hospital ou a atualizar uma infraestrutura crítica, como uma central elétrica?

A História mostra que nenhum sistema é completamente seguro – no entanto, algumas proteções e metodologias são mais seguras do que outras. O desafio é conseguir identificar as melhores opções.

DEFESA CONTRA ATAQUES INFORMÁTICOS

Ao planear um novo sistema de Gestão Técnica ou um projeto de uma infraestrutura, como identificar as opções de tecnologia segura?

Tudo começa com a seleção dos componentes necessários ao projeto, altura em que é necessário responder a uma questão essencial: Esta tecnologia foi projetada com a cibersegurança em mente desde o início? Ou essas preocupações foram simplesmente uma reflexão tardia, e feitos acrescentos quando o produto estava prestes a ser comercializado?

É necessária transparência para que este processo de seleção seja baseado em factos – em vez de deixar que os integradores e clientes interpretem linguagens comerciais que nem sempre são qualificadas nem justificadas.

A cibersegurança é uma necessidade fundamental em todo o desenvolvimento de tecnologia. Deve ser levada em conta desde o início do processo de conceção, e deve ser incorporada em todos os aspetos da função e do objetivo do produto.

É por isso essencial uma norma objetiva para medir e verificar a maturidade e a segurança do ciclo de desenvolvimento de um produto. Quando se verifica que o desenvolvimento de um produto segue as melhores práticas e as normas estabelecidas, os clientes podem confiar que esses produtos passaram por testes de segurança rigorosos.

Isto cria confiança nos clientes e utilizadores, ao confirmar que o fabricante do produto:

- Identificou fragilidades e vulnerabilidades de segurança no início da conceção do produto.
- Geriu o risco, utilizando uma análise cuidada para identificar riscos, e depois priorizou e corrigiu esses riscos.
- Compriu com as versões mais recentes das normas e regulamentos de segurança aplicáveis.
- Mediu o seu progresso em relação às normas de desenvolvimento seguro e usou essas métricas para avançar na maturidade de segurança do seu ciclo de vida de desenvolvimento de produto.

NORMAS ISA/IEC 62443		
GERAL	**ISA-62443-1-1**	Conceito e modelos
	ISA-TR62443-1-2	Glossário de termos e abreviaturas
	ISA- 62443-1-3	Métricas de conformidade de segurança do sistema
	ISA- TR62443-1-4	Ciclo de vida e casos de uso da segurança IACS
POLÍTICAS E PROCEDIMENTOS	**ISA-62443-2-1**	Requisitos para um sistema de gestão de segurança IACS
	ISA-TR62443-2-2	Guia de implementação de sistemas de gestão de segurança IACS
	ISA-TR62443-2-3	Gestão de correções em ambiente IACS
	ISA-TR62443-2-4	Requisitos para fornecedores de soluções IACS
SISTEMA	**ISA- TR62443-3-1**	Tecnologias de segurança para IACS
	ISA-62443-3-2	Avaliação de riscos de segurança e conceção de sistema
	ISA-62443-3-3	Requisitos de segurança do sistema e níveis de segurança
COMPONENTE	**ISA-62443-4-1**	Requisitos de desenvolvimento de produto
	ISA-62443-4-2	Requisitos técnicos de segurança para componentes IACS

NORMAS DE DESENVOLVIMENTO SEGURO: ISA/IEC 62443

O processo de conceção é essencial para o sucesso – ou fracasso - da cibersegurança de um produto. Então, o que é um "bom" processo de desenvolvimento?

Esta é uma questão que a indústria tecnológica tem colocado continuamente, o que levou a International Society of Automation (ISA) a formar uma equipa de especialistas em segurança que pudesse propor critérios oficiais que configurem boas práticas nas tecnologias de automação e sistemas de controlo. As normas criadas por esta equipa foram adotadas internacionalmente pela Comissão Eletrotécnica Internacional (IEC) e são reconhecidas por um número crescente de governos a nível mundial.

Este conjunto de normas – conhecido como ISA/IEC 62443 – cobre todo o processo de desenvolvimento de produtos de tecnologia operacional (OT) utilizada em sistemas de automação e controlo. Rapidamente se tornou a norma seguida para garantir a cibersegurança de um produto nos setores industrial e de automação, bem como noutros setores.

Entre os documentos que fazem parte da família completa das normas ISA/IEC 62443 (Figura 2), um deles foca-se no processo de desenvolvimento do produto, definindo como esse processo deve abordar a cibersegurança de modo a criar um processo de desenvolvimento de produto seguro. Essa norma é a ISA/IEC 62443-4-1.

PROCESSO DE DESENVOLVIMENTO SEGURO

A Honeywell tem-se baseado na norma ISA 62443-4-1 há muitos anos, bem como noutras normas aplicáveis para desenvolver de forma segura os seus produtos tecnológicos.

Por exemplo, os produtos de Gestão Técnica de Edifícios Honeywell também utilizam a ISA/IEC 62443- 4-2 como referência para os requisitos de segurança dos componentes, e a ISA/IEC 62443-3-3 para sistemas completos.

Desta forma, a adesão da Honeywell à família de normas ISA/IEC 62443 oferece aos integradores e clientes que têm de escolher tecnologias de gestão técnica de edifícios um elevado nível de confiança de que os seus produtos não se limitam a alegar que são resistentes a ataques informáticos – eles foram concebidos, testados e validados para cibersegurança desde o início.

Mas isto levanta outra questão: Quando um fabricante como a Honeywell alega seguir um processo de desenvolvimento seguro, como podem os clientes saber se isso é verdade, e se isso foi feito de forma eficaz? Respondemos de seguida a essa questão.

CICLO DE DESENVOLVIMENTO SEGURO: CERTIFICAÇÃO DO PROCESSO

O passo seguinte na construção de transparência e confiança é fornecer provas de que as empresas que alegam seguir um processo reconhecido estão de facto a fazê-lo.

Para corresponder a esta necessidade, foi definido um processo de certificação em conjunto com as normas internacionais, incluindo a ISA e a IEC.

Foram fundadas várias empresas de auditoria para examinar de forma independente empresas que pretendam seguir os processos ISA/IEC 62443.

O ponto de partida é o ciclo de desenvolvimento seguro propriamente dito, pelo que a primeira etapa de certificação é a certificação do processo (ISA/IEC 62443-4-1).

Para obter esta certificação, um auditor independente avalia o ciclo de desenvolvimento seguro da empresa que pretende obter a certificação. O auditor conduz uma avaliação profunda dos processos da empresa e compara-os com as exigências na norma ISA/IEC 62443. São selecionados projetos aleatoriamente, que são depois inspecionados para reunir provas de que estão de facto a ser seguidos processos adequados de forma correta. Isto não é um pequeno exercício – a certificação pode demorar meses.

Se a avaliação for positiva, é atribuída a Certificação de Processo ISA/IEC 62443, indicando que a norma está a ser seguida para manter um ciclo de desenvolvimento seguro. Esta certificação é depois publicada no site ISASecure para a tornar acessível publicamente.

A divisão Honeywell Building Technologies (HBT) completou o processo de Certificação ISA 62443-4-1 e foi-lhe atribuído o certificado em janeiro 2023. O certificado pode ser consultado aqui.

Esta certificação significa que os clientes da Honeywell podem ter a certeza de que os seus produtos foram desenvolvidos de acordo com as normas internacionais e da indústria para cibersegurança, e que isso foi confirmado de forma independente.

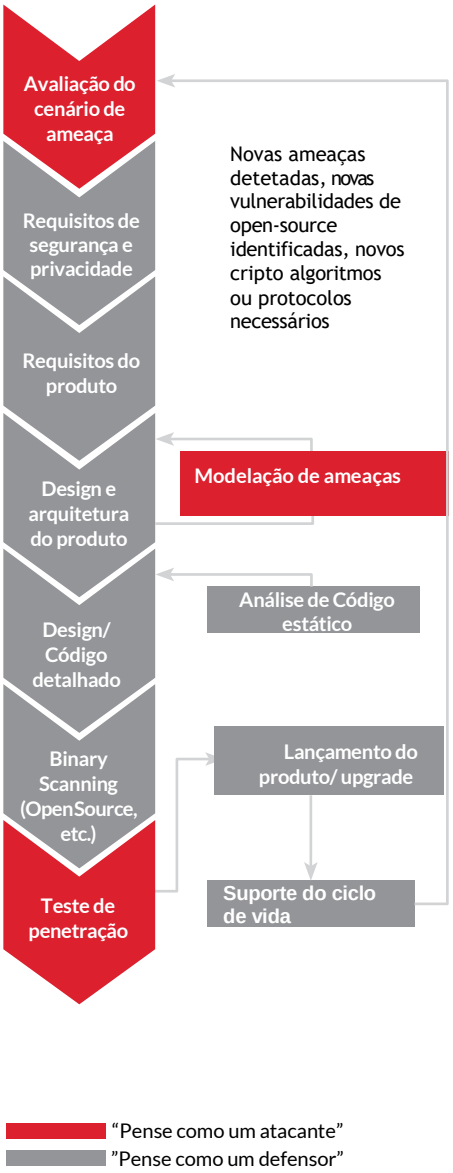

Figura 2: Exemplo de um Ciclo de Desenvolvimento Seguro baseado nas normas internacionais como a ISA/IEC 62443

Honeywell Building Technologies
715 Peachtree St NE
Atlanta, Georgia 30308
buildings.honeywell.com

THE FUTURE IS WHAT WE MAKE IT

Honeywell