Segurança cibernética

Riscos e ameaças cibernéticas para ambientes operacionais de missão crítica

pwc

Ambientes operacionais e missão crítica

Sistemas de missão crítica (*Operational Technology* – OT) são combinações de componentes de tecnologia como softwares, hardwares, bancos de dados, processos e aplicativos que desempenham uma função essencial para o funcionamento e manutenção de operações e processos críticos. Esses sistemas estão presentes na sociedade e se expandem à medida que as organizações avançam em sua transformação digital.

Veja exemplos de ambientes de missão crítica:

Energia e *utilities*

- **Óleo e gás:** caldeiras, sensores de pressão, perfuração/telemetria de perfuração, estabilização de plataformas e detecção de vazamentos
- **Energia:** turbinas eólicas, barragens de água, fazendas solares, usinas nucleares, gás natural e carvão
- **Química:** fornos, sensores de pressão de gás e dutos
- **Mineração:** veículos autônomos, perfuradoras, sensores de colapso e de alarmes, sensores de qualidade do ar e da água, e iluminação

Produção industrial

- **Alimentos e bebidas:** fornos, fritadeiras, caldeiras, atuadores, engarrafadores, esteiras transportadoras e paletizadores
- **Automotivo/industrial:** montagem, pintores, transportadores e robôs de manuseio de materiais
- **Eletrônica:** sala limpa BMS (*Building Management System*), HMI (*Human Machine Interface*) e controladores

Saúde

- **Dispositivos médicos:** marca-passos, bombas de insulina e monitores de pacientes
- **Produtos farmacêuticos:** braços robóticos, refrigeradores e empacotadores
- **Sistemas de gerenciamento de edifícios:** HVAC/filtragem de ar, iluminação, supressão de incêndio e controle de acesso
- **Equipamento cirúrgico ou de laboratório:** instrumentos robóticos, *scanners* de imagem e dispensadores farmacêuticos

Transporte e logística

- **Locomotiva:** troca de trilhos, detectores de defeito, sensores de altura/largura, sensores de distribuição de peso, sistemas de controle e frenagem
- **Aeroespacial/marítimo:** piloto automático, controle de segurança e de direção, propulsão, controle de flutuabilidade e gerenciamento portuário
- **Varejo:** transportadores, paletizadores, manipuladores de materiais, separadores, refrigeradores e gerenciamento de edifícios

Atenção aos riscos cibernéticos

A tecnologia operacional é anterior à era dos sistemas de informação. Inicialmente, ela consistia em sistemas isolados que executavam funções de controle em hardware/software especializado e protocolos de comunicação. Esses sistemas foram substituídos pelos mesmos produtos e serviços já em uso no domínio da tecnologia da informação tradicional.

A transformação digital, associada à necessidade de dados nas empresas (especificamente para o planejamento de recursos), exigiu a conexão de sistemas e uma transferência de dados mais eficaz. Para sistemas de missão crítica, conectar sistemas legados que ainda não haviam sido expostos à rede corporativa gera novos riscos.

Dados de instalações OT

- Dados de produção
- Garantia de qualidade de produção
- Inventário
- Suprimentos
- Estratégia de manutenção

+

***Enterprise Resource Planning* (ERP)**

- Vendas
- CRM
- Compras
- Financeiro
- Recursos Humanos

=

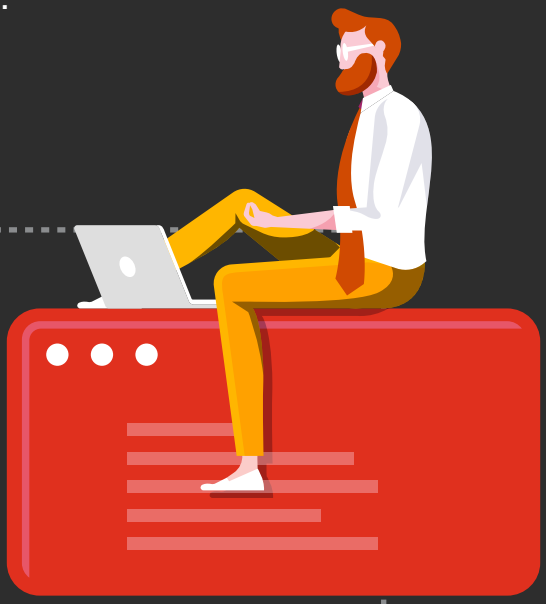
Aumento de eficiência

Integração: a conectividade e a transformação são vistas com mais urgência após vários incidentes em todo o mundo. Elas atuaram como um impulsionador de mais segurança no ambiente de OT. Muitas organizações estão vendo esse desafio como uma oportunidade para alinhar operações, TI e segurança da informação a fim de aumentar a segurança dos ambientes operacionais e reduzir riscos para a organização.

Impacto nas organizações

A indústria global tem sido abalada por ataques cibernéticos que afetam os ambientes operacionais. Com o aumento da frequência e da gravidade desses incidentes, o custo para as empresas em termos de receitas perdidas e remediação continuará crescendo.

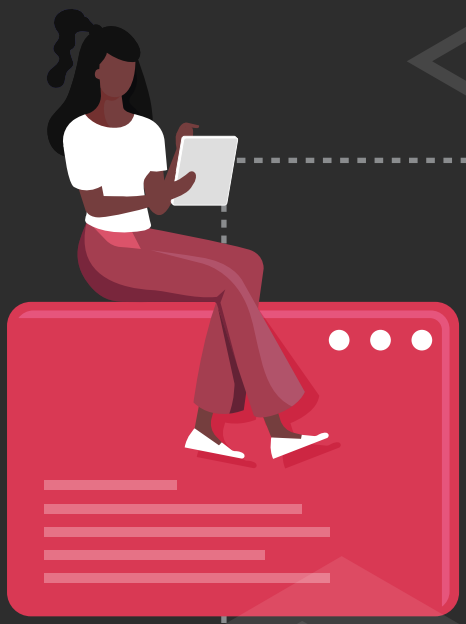
Conheça alguns casos:



2010
Stuxnet

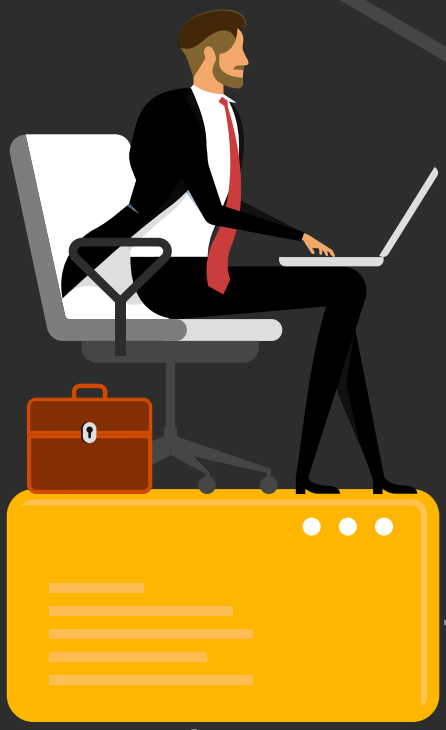
Malware sofisticado projetado para atacar controladores lógicos programáveis de processos eletromecânicos de centrífugas nucleares em uma instalação de enriquecimento de urânio no Irã.

Aproveitou vários *exploits* de dia "zero" e certificados digitais roubados para replicar e atingir seus objetivos destrutivos. Considerado o primeiro *malware* específico de OT de seu tipo.



2011
Duqu/Flame/Gauss

Três tipos de *malware* projetados para coletar informações existentes em sistemas de controle, provavelmente para fins de reconhecimento. O Flame utilizou microfones, câmeras web, registro de teclas pressionadas e geolocalização de imagens para roubar informações.



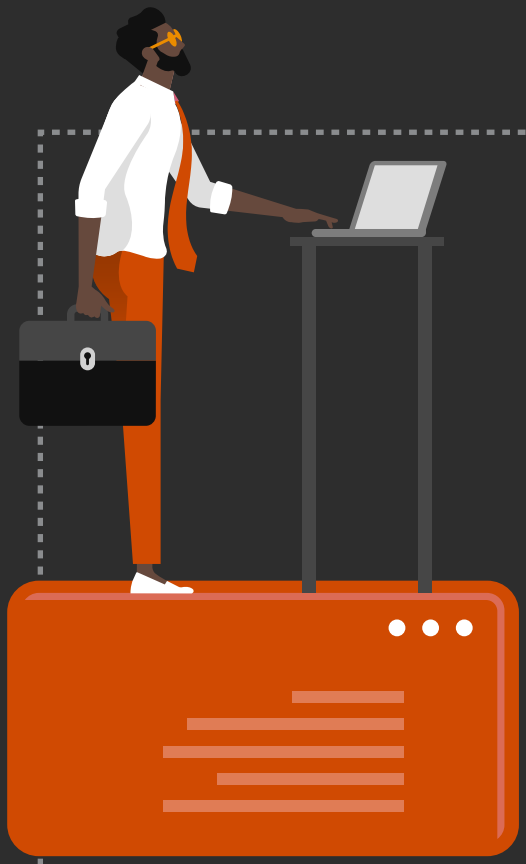
2013
HAVEX

Malware modular para coleta de informações, mas expansível remotamente para executar outras funções. Representa a evolução da influência geopolítica no ciberespaço, especificamente no que diz respeito à infraestrutura crítica.

2015 e 2016
BlackEnergy/CRASHOVERRIDE

O primeiro ataque cibernético confirmado publicamente capaz de impactar uma rede elétrica ocorreu em 2015 e deixou cerca de 250 mil pessoas sem energia na Ucrânia. Um segundo ataque foi realizado com efeito semelhante no ano seguinte.

Ataques sofisticados contra sistemas de controle foram combinados com ataques contra centrais de atendimento telefônico para atrasar a informação de problemas e a coordenação da resposta.



2017
NotPetya

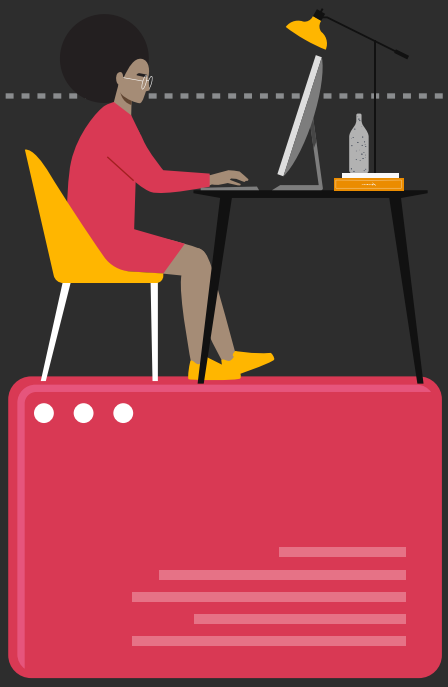
Uma empresa farmacêutica multinacional foi afetada por um ataque global do *malware* NotPetya que criptografou muitos de seus sistemas de computador. O incidente causou perda de produção e receita, interrompendo as operações em todo o mundo (estimativa de US$ 1 bi em danos).

Uma empresa global de bens de consumo também foi vítima do *malware* NotPetya, que inibiu sua capacidade de enviar faturas, causando uma queda de 3% na receita (estimativa de US$ 100 milhões em danos).

2017
Trisis/Triton

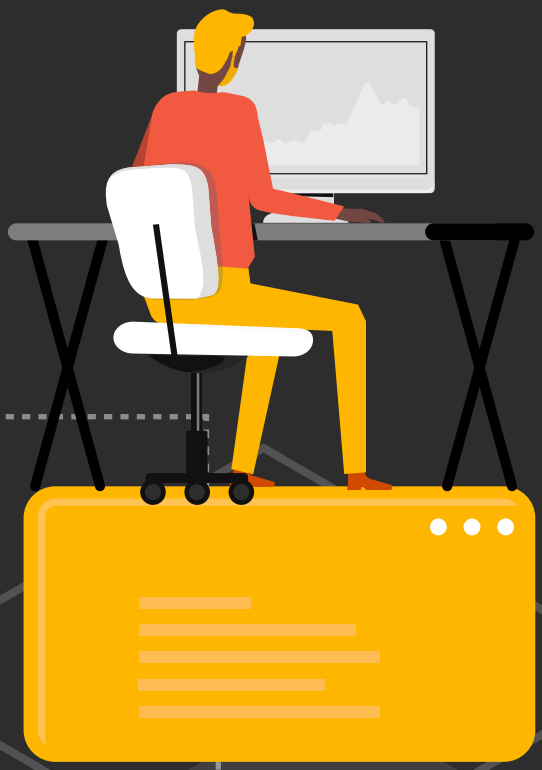
Projetado especificamente para os sistemas de segurança da organização-alvo, permite que o invasor provoque situações perigosas potencialmente fatais ou fisicamente destrutivas.

É o primeiro *malware* desse tipo conhecido a visar sistemas de segurança.



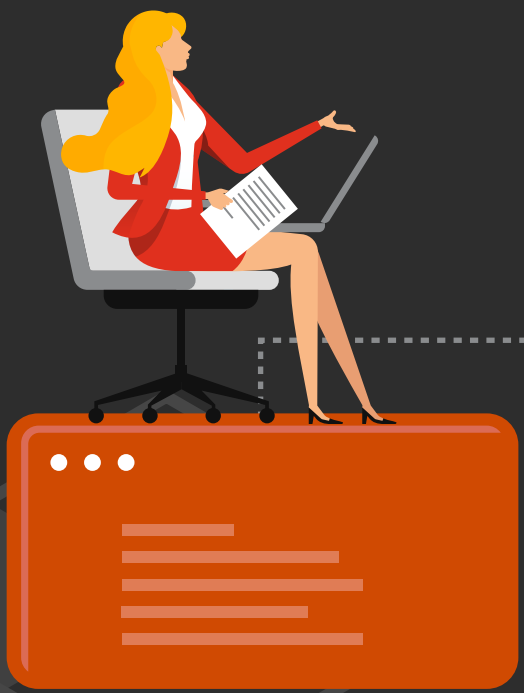
2019
LockerGoga

Paralisou as operações de uma empresa de energia renovável, causando um impacto financeiro de cerca de US$ 35 milhões na primeira semana. Os custos gerais para essa empresa de são estimados em aproximadamente US$ 75 milhões.



2020
Ekans

Operações interrompidas em várias instalações de grandes fabricantes de automóveis e em unidades farmacêuticas de uma empresa de saúde.



2021
Darkside

Operações da principal fornecedora de combustíveis e oleodutos dos Estados Unidos foram atacadas em 2021, causando escassez de combustível em 13 estados.

Como podemos ajudar

As empresas precisam adotar uma postura de segurança proativa para gerenciar programaticamente o risco de segurança cibernética para seus sistemas operacionais. A PwC oferece uma gama de serviços para a adoção de programas integrados de segurança de TI e OT que permitem reduzir riscos para as organizações.

Segurança para OT

Programa de segurança cibernética

Programa de proteção baseado em ativos, com foco em riscos de negócio e com clareza de funções, responsabilidades e governança.

Aferição da maturidade de segurança

Diagnóstico robusto apoiado pelas melhores práticas para avaliar a maturidade atual e criar o programa de segurança cibernética de missão crítica.

Remediação e avanço da maturidade

Desenvolvimento de ações estratégicas, táticas e operacionais para evolução dos controles de proteção e da maturidade.

Conformidade em Segurança Cibernética

Apoio na identificação de oportunidade e planos de ações frente aos requisitos regulatórios emergentes para o setor, orientados a segurança cibernética.

Cyber Due Diligence

Visão rápida dos principais riscos de ativos e dados que estão sendo adicionados ao ambiente em uma transação.

Plano de crise e resposta aos incidentes cibernéticos

Investigação e suporte adequado para isolar atividades cibernéticas anômalas que afetam as operações e responder a elas.

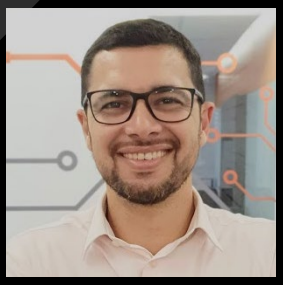
Gestão de risco continuada com monitoramento de segurança

Ferramentas de detecção e monitoramento projetadas para as operações industriais com visibilidade dos riscos.

Contatos

Ronaldo Valiño
Sócio e líder da
Indústria de Energia
ronaldo.valino@pwc.com

Eduardo Batista
Sócio e Líder de *Cyber Security* no Brasil
eduardo.batista@pwc.com



Magnus Santos
Sócio de *Cyber Security*
para a Indústria de Energia
magnus.santos@pwc.com

Larissa Escobar
Diretora de *Cyber Security*
para a Indústria de Energia
larissa.escobar@pwc.com

PwC Brasil @PwCBrasil PwC Brasil @PwCBrasil PwC Brasil @PwCBrasil

(DC0) Informação Pública
Versão: Junho 2021 | [F301]