Empresas & Negócios

Matéria de capa

blackdovfx_CANVA

SEGURANÇA

ATAQUES CIBERNÉTICOS PODERÃO USAR TECNOLOGIA PARA FERIR OU MATAR HUMANOS

Leia na página 6

O Gartner, Inc., líder mundial em pesquisa e aconselhamento para empresas, alerta que, até 2025, os cibercriminosos serão capazes de atacar ambientes de tecnologia operacional (OT) com intenção real de ferir ou matar humanos.

Ataques a ambientes de OT (com estruturas com hardware e software dedicados a monitorar ou controlar equipamentos, ativos e processos) estão se tornando a cada dia mais comuns.

As invasões também evoluíram de iniciativas que representavam apenas a interrupção imediata do processo, como o desligamento de um equipamento, para o comprometimento de toda a integridade dos ambientes empresariais e industriais com a intenção de causar grandes danos físicos. Outros eventos recentes, como o ataque com o ransomware Colonial Pipeline, destacaram a necessidade de ter redes diferentes e devidamente segmentadas para TI e OT.

"Em ambientes operacionais, os líderes de segurança e gerenciamento de risco devem se preocupar mais com os perigos do mundo real para os humanos e o meio ambiente, em vez de focar apenas o roubo de informações", diz Wam Voster, Diretor de Pesquisa Sênior do Gartner. "Consultas com clientes de diversos portes revelam que organizações em setores com uso intensivo de ativos, como manufatura, recursos e serviços públicos, precisam trabalhar para definir estruturas de controle apropriadas".

De acordo com o Gartner, incidentes de segurança em ambientes de tecnologia operacional e outros sistemas ciberfísicos (CPS - Cyber-Physical Systems) têm três motivações principais: dano real, vandalismo comercial (produção reduzida) e vandalismo de reputação (tornando uma marca não-confiável).

O Gartner prevê que o impacto financeiro dos ataques a CPS resultando em vítimas fatais chegará a mais de US$ 50 bilhões até 2023. Mesmo sem levar em conta o valor da vida humana, os custos para as organizações em termos de compensação, litígio, seguro, multas regulatórias e perda de reputação será significativo. As análises também indicam que a maioria dos CEOs será pessoalmente responsável por tais incidentes.

O Gartner recomenda que as organizações adotem uma estrutura de dez controles de segurança para melhorar a postura de segurança em suas instalações e evitar que incidentes no mundo digital tenham um efeito adverso no mundo físico.

1 **Defina funções e responsabilidades** – Nomeie um gerente de segurança da OT para cada instalação. Este profissional é responsável por atribuir e documentar funções e responsabilidades relacionadas à segurança para todos os trabalhadores, gerentes seniores e quaisquer terceiros.

2 **Garanta treinamento e conscientize funcionários** – Todos os colaboradores alocados em uma planta de OT devem ter as habilidades necessárias para suas funções. Os funcionários de cada instalação devem ser treinados para reconhecer os riscos de segurança, os vetores de ataque mais comuns e o que fazer em caso de um incidente de segurança.

3 **Implemente e teste a resposta a incidentes** – Garantir que cada instalação implemente e mantenha um processo de gerenciamento de incidente de segurança específico para OT, em um plano que inclui quatro fases: preparação; detecção e análise; contenção, erradicação e recuperação; e atividade pós-incidente.

4 **Faça backup e tenha sistemas de restauração e recuperação de dados em caso de desastres** – Certifique-se de que os procedimentos adequados de backup, restauração e recuperação de desastres estejam em vigor. Para limitar o impacto de eventos físicos, como incêndio, não armazene mídia de backup no mesmo local que o sistema de backup. A mídia de backup também deve ser protegida contra divulgação não autorizada ou uso indevido. Para lidar com incidentes de alta gravidade, deve ser possível restaurar o backup em um novo sistema ou máquina virtual.

5 **Gerencie mídias portáteis** – Crie uma política para garantir que todas as mídias portáteis de armazenamento de dados, como pen drives e computadores portáteis, sejam verificadas, independentemente do dispositivo pertencer a um funcionário interno ou a terceiros, como subcontratados ou representantes do fabricante do equipamento. Apenas a mídia considerada livre de código ou software malicioso pode ser conectada ao ambiente das empresas.

6 **Tenha um inventário de ativos atualizado** – O gerente de segurança deve manter um inventário continuamente atualizado de todos os equipamentos e programas ligados à rede da planta de operação tecnológica.

7 **Estabeleça a segregação de rede adequada** – As redes OT devem ser fisicamente ou/e logicamente separadas de qualquer outra rede, tanto interna quanto externamente. Todo o tráfego de rede entre um OT e qualquer outra parte da rede deve passar por uma solução de gateway seguro como uma zona desmilitarizada (DMZ). As sessões interativas para OT devem usar autenticação multifator para autenticar no gateway.

8 **Colete registros e implemente a detecção em tempo real** – Políticas ou procedimentos apropriados devem estar em vigor para registro automatizado e revisão de eventos de segurança reais e potenciais. Isso deve incluir tempos de retenção claros para os logs de segurança a serem retidos e proteção contra adulteração ou modificação indesejada.

9 **Implemente um processo de configuração seguro** – As configurações seguras devem ser desenvolvidas, padronizadas e implantadas para todos os sistemas aplicáveis, como terminais, servidores, dispositivos de rede e dispositivos de campo. O software de segurança de endpoint, como o antimalware, deve ser instalado e ativado em todos os componentes do ambiente OT que o suportam.

10 **Crie um processo formal de patching** – Implemente um processo para que os patches sejam qualificados pelos fabricantes de equipamentos antes da implantação. Depois de qualificados, os patches só podem ser implantados em sistemas apropriados com uma frequência pré-especificada.

Fonte e outras informações: (www.gartner.com).

EMPREENDEDORES COMPULSIVOS

#tenhacicatrizes

Oportunidades

Claudio Zanutim (*)

Com tantas mudanças disruptivas, e principalmente diante de tantas evoluções no mercado de trabalho, um mercado que vem enfrentando grandes transições entre "ocupação e localização", faz com que tudo seja mais competitivo para nós, e exige que sejamos profissionais assertivos, e até mesmo, empreendedores que se auto lideram. Mas você sabe exatamente o que isso significa?

Muito se tem falado sobre assertividade, mas muita gente ainda ignora o que isso representa. Trata-se também de:

- Ter uma visão superior sobre todas as etapas de produção de uma organização;
- Se antecipar a possíveis falhas no sistema;
- Preparar-se para resolver qualquer imprevisto sem prejuízo do trabalho em execução.

Resumindo, ser assertivo é principalmente, estar pronto para resolver qualquer problema que surgir.

Por sua vez, ser empreendedor tem a ver ainda, com **identificar oportunidades** no mercado, notando o que o cliente quer, diferenciando o produto ou serviço de que ele necessita.

Para o legítimo empreendedor (o executivo raiz), não é difícil identificar as oportunidades para chegar aos seus objetivos, preenchendo as possíveis lacunas do mercado com novas ideias ou ofertas de produtos e serviços. O empreendedor assertivo tem uma percepção apurada, por isso, pode reconhecer e agir sobre as oportunidades do mercado atual, inovando em cima disso e de suas ações.

Por ter uma visão à frente de sua época, e conseguir enxergar além dos demais, o empreendedor assertivo traz sempre consigo novos *insights*, cria oportunidades ou simplesmente uma maneira melhor de fazer algo trivial.

No ambiente competitivo, o empreendedor assertivo é o pioneiro das oportunidades, mesmo tendo em mente que em cada uma delas existirão obstáculos a serem superados.

A boa notícia é que existem ferramentas que podem lhe auxiliar a isso, acompanhe;

A matriz SWOT

O estudo da avaliação SWOT (Strenghts, Weaknesses, Oportunities, Threat) é realizado para identificar pontos internos e externos, apontando as oportunidades que poderão ser desenvolvidas em potencial. Com a matriz SWOT, a organização poderá identificar as forças, fraquezas, ameaças e oportunidades.

- As forças podem ser como os recursos disponíveis;
- As fraquezas podem ser também recursos não administrados e todas as falhas que não levam ao aperfeiçoamento em um determinado segmento.
- As oportunidades compreendem tudo que favoreça e venha somar na estrutura, na qualidade e no crescimento da organização,
- As ameaças podem ser compreendidas como tudo o que leva risco para alcançar as metas e objetivos da empresa.

O objetivo da avaliação é relacionar os pontos fortes e fracos internos da organização com as oportunidades e ameaças externas do mercado e da concorrência.

Contudo, antes de se criar uma matriz SWOT é importante fazer uma avaliação do ambiente, que permitirá identificar as variáveis internas e externas, que impactam a organização, identificando riscos e oportunidades no presente e também no futuro.

Depois de identificar as principais ameaças e oportunidades, forças e fraquezas, podemos especificar nosso negócio com base em quatro elementos:

1. Uma empresa ideal é elevada em termos de oportunidades e baixa em termos de ameaças;
2. Uma empresa especulativa é elevada tanto em termos de oportunidades como de ameaças;
3. Uma empresa madura é baixa em termos de oportunidades e também em ameaças;
4. Uma empresa arriscada é baixa em termos de oportunidades e alta em ameaças.

Após essa avaliação é possível criar uma matriz SWOT da seguinte forma:

1. Classificar os fatores fortes identificados em dois grupos: (A) os que estão associados a oportunidades potenciais ou ameaças, (B) e os que não estão associados;
2. Dividir os pontos fracos da mesma forma;
3. Criar uma matriz com quatro quadrantes;
4. Unir os pontos fortes e fracos, juntamente com as oportunidades e ameaças, em cada quadrante.

Não se engane, *insights* não são oportunidades

Ao contrário do que algumas pessoas imaginam, uma ideia de negócio não significa uma oportunidade de negócio. Que isso fique claro! Um *insight* só se transforma em oportunidade quando seu propósito vai ao encontro de uma necessidade do mercado.

Neste exato momento, cerca de 450 pessoas estão tendo a mesma ideia, porém, apenas três delas a colocarão em prática e criarão algo novo para o mercado, ou algo que atenda uma necessidade. Mas essas pessoas que terão novas ideias, devem, antes de tudo, identificar o tempo oportuno para realizar.

Oportunidades também têm o tempo certo para acontecer. Conseguindo traduzir as necessidades do mercado e sendo uma grande oportunidade; ainda assim, corre-se o risco de em apenas 12 meses depois dele ser lançado, cair no esquecimento. É o que chamamos de sucesso passageiro.

Claudio Zanutim

Claro que tudo isso, envolve uma sequência de ações, como a organização estar preparada para constantemente melhorar e atualizar os seus produtos, aproveitando todas as oportunidades de aperfeiçoamento que surgirem. No entanto, isso também pede que o vendedor tenha sempre uma postura e visão empreendedora.

O que isso significa na prática? Que o profissional precisará participar de várias atividades que permitam sua atualização e conhecimento, como por exemplo: treinamentos, consultorias, workshops, lives, cursos, seminários e leituras. É preciso compreender as tendências, se adaptar às transições, ser flexíveis às mudanças e as situações econômicas, políticas e até sociais do mercado. Com este hábito adquirido, garantidamente surgirão muitas novas ideias para melhorar o seu negócio, os seus resultados e as suas metas. Criando oportunidades.

(*) É Membro dos Empreendedores Compulsivos, Palestrante e Trainner Internacional. Mais 150 mil pessoas treinadas. Auxilia empresas e pessoas na maximização da performance em vendas e no atingimento de objetivos e metas. Autor de 7 livros, 3 e-books e dez artigos acadêmicos, é reconhecido nos meios empresarial, acadêmico e popular, principalmente com o Best Seller: Como Construir Objetivos e Metas Atingíveis.