Cibersegurança Portuária

MARITIME LAW ACADEMY®

Bruno Eduardo Budal Lobo

Advogado (OAB/SC nº 30.059), Mestrando da Universidade Católica de Brasilia – UCB, Especialista em Direito Aduaneiro e Comércio Exterior pela Universidade do Vale do Itajaí - UNIVALI, Presidente da Comissão Estadual de Direito Aduaneiro da OAB/SC, Coordenador do Curso de Pós-Graduação lato sensu em Direito Aduaneiro e Tributário Internacional da Maritime Law Academy, possui cursos de Formação como Despachante Aduaneiro e de Analista em logística internacional pelas Associação Brasileira de Comércio Exterior - ABRACOMEX

MARITIME LAW ACADEMY®

Tópico I
Onde estamos com esse assunto?

Notícias

Persiste incidente 'grave' de cibersegurança em portos na Austrália

AFP

12/11/2023 03h53

Agências do governo australiano fizeram uma reunião de crise neste domingo (12) para responder a um incidente de segurança cibernética "grave e em curso" que interrompeu as operações nos principais portos do país.

Na sexta-feira, a operadora portuária DP World interrompeu as conexões de Internet nos portos de Sydney, Melbourne, Brisbane e Fremantle para impedir "qualquer acesso não autorizado em curso" à sua rede, de acordo com um porta-voz.

É um incidente "grave e está em curso", disse neste domingo a ministra do Interior e de Cibersegurança, Clare O'Neil, na plataforma X.

"A DP World administra quase 40% das mercadorias que entram e saem do nosso país", acrescentou.


José Paulo Kupfer
Copom erra, expõe racha político e eleva incertezas

OPINIÃO

Artigo - Ataques cibernéticos no setor portuário: custos para eliminar riscos são investimento

Alex Gatto com colaboração de Carlos Albuquerque 15/03/2023 - 18:08

Os terminais portuários são locais críticos para o comércio internacional, com um grande número de navios e cargas movimentando-se diariamente. No entanto, com a crescente dependência da tecnologia da informação, os terminais estão se tornando cada vez mais vulneráveis aos ataques cibernéticos. As consequências podem ser graves, como atrasos nas operações, perda de dados, roubo de informações confidenciais e, até mesmo, a interrupção total do comércio marítimo. Além disso, a segurança dos navios em trânsito também pode ser comprometida, colocando em risco a vida humana e o meio ambiente.

Por que trocar o maquinário portuário?

O investimento será centrado na produção nacional dos guindastes de carga, com o objetivo de proteger a segurança nacional, que parece estar ameaçada pelo uso de software chinês muito avançado, amplamente utilizado nos portos norte-americanos.

Com o projeto de fabricação dos guindastes em solo estadunidense, também serão implementadas novas diretrizes sobre a segurança da Guarda Costeira dos EUA exigindo requisitos de segurança digital para guindastes estrangeiros que estão implantados em portos marítimos estratégicos.

Um outro ponto é o cumprimento de uma ordem executiva do presidente Biden, que estabelece padrões básicos de **segurança cibernética** para redes de computadores implantadas nos portos norte-americanos.

SEGURANÇA E PRIVACIDADE

EUA investirá bilhões em guindastes para melhorar cibersegurança

O governo estadunidense planeja investimento bilionário para fabricar guindastes por lá em prol da cibersegurança dos portos; entenda

Pedro Spadoni | 23/02/2024 08h47

Para quem tem pressa:

- A administração do presidente dos EUA, Joe Biden, emitiu, nesta semana, diretrizes de cibersegurança para proteger os portos marítimos dos EUA, com foco em vulnerabilidades e no uso de guindastes fabricados na China;
- Mais de US$ 20 bilhões (R$ 1 trilhão) serão investidos em infraestrutura portuária, incluindo a fabricação de guindastes nos EUA, para diminuir riscos de cibersegurança e dependência de equipamentos chineses;
- Há uma preocupação específica com guindastes fabricados na China, que representam cerca de 80% do mercado em portos estadunidenses. Novos requisitos de cibersegurança serão impostos para mitigar riscos de espionagem ou disrupções operacionais por hackers;
- Além disso, a Guarda Costeira dos EUA conduzirá inspeções e imporá a obrigatoriedade de relatos de ciberataques em navios e instalações portuárias, como parte das ações para prevenir ataques que possam comprometer as cadeias de suprimentos e a infraestrutura crítica.

EUA acham dispositivos de espionagem chinês em portos americanos

Modems com acesso à rede celular instalados nas gruas podem ter sido usados para a coleta de dados de inteligência

Por Dustin Volz — Dow Jones Newswires, de Washington

08/03/2024 05h01 · Atualizado há 2 meses

Uma investigação do Congresso sobre guindastes de carga feitos na China e instalados em portos nos EUA encontrou equipamentos de comunicação que não parecem destinados a operações normais, alimentando preocupações de que as máquinas estrangeiras possam representar um risco secreto para a segurança nacional.

Os componentes interceptados em alguns casos incluem modems celulares que podem ser acessados remotamente, segundo assessores e documentos do Congresso.

Cibersegurança: ataques no setor portuário acendem alerta sobre proteção dos dados

- julho 21, 2023

Ataque em porto do Japão reforça importância de investir em cibersegurança

Pensar na segurança da informação tem sido essencial para que as empresas garantam a proteção dos milhões de dados que são gerados diariamente. No setor portuário, os ataques cibernéticos que vem ocorrendo mundialmente alertam sobre a importância de portos e terminais investirem em cibersegurança.

O caso mais recente aconteceu no início de julho, quando o Porto de Nagoya, maior e mais movimentado porto do Japão, foi alvo de um ataque de ransomware, afetando a operação nos terminais de contêineres, que foi interrompida por dois dias.

O ransomware é um malware (software malicioso) responsável por criptografar arquivos no armazenamento local ou de rede com senha, momento em que os hackers exigem um resgate para devolver os dados às empresas. Isso gera enormes prejuízos financeiros aos portos e graves interrupções na circulação das mercadorias.

De acordo com o engenheiro de software, professor universitário e diretor da T2S, Rodrigo Salgado, esse tipo de ataque vem sendo comum. “Pedem o resgate mediante a entrega dos dados, mas não é garantido que vão devolver o que foi sequestrado. Normalmente as empresas só percebem a importância de investir em cibersegurança quando sofrem com isso”, comenta.

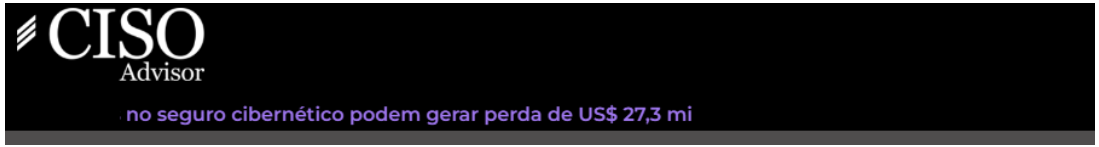
portosenavios

HOME | NOTÍCIAS | ARTIGOS | REVISTA | SERVIÇOS

PORTOS E LOGÍSTICA

Cibersegurança: maturidade do setor portuário é considerada baixa, de acordo com especialistas

Bianca Guilherme 18/01/2023 - 00:15



Em entrevista à agência, Hodges disse que a defesa cibernética é tão importante quanto a defesa antimísseis.

O ex-general também lembrou o ataque do ransomware NotPetya em 2017, que atingiu várias empresas em diferentes países, incluindo a principal transportadora de cargas do mundo, a dinamarquesa Maersk. A Maersk teria tido um prejuízo da ordem de US$ 300 milhões como consequência do ataque.

"Bremerhaven e Hamburgo são de fato os portos marítimos mais importantes dos quais a aliança depende, em termos de equipamento militar, não apenas de carga comercial... Se não pudermos usar Bremerhaven, será muito difícil para os EUA fornecer reforços e realizar uma parte dos planos operacionais ", disse Hodges.

Além disso, o general está preocupado com a decisão de Berlim de permitir que a companhia marítima estatal chinesa Cosco compre uma participação no terminal do maior porto da Alemanha, Hamburgo. Segundo Hodges, a China terá acesso à infraestrutura crítica de transporte e, se desejar, poderá causar danos.

Tópico II

O que é possível ser feito?

Cibersegurança Portuária

- Estrutura (framework) de trabalho
  - International Association of Ports and Harbors - IAPH
  - Cibersecurity Guidelines for Ports and Port Facilities

Cibersegurança Portuária

- Artigo:
  - Cibersegurança Portuária e Ameaças: Um modelo estrutural para prevenção e desenvolvimento de políticas
    - Chalermpong Senarak
    - Departamento de ciências náuticas e logítica marítima, Faculdade de Estudos Marítimos Internacionais – Universidade de Kasetsart
    - The Asian Journal of Shipping and Logistics

Table 3
Characteristics of cyberthreat.

Cyberthreat category	Objective	Cyberthreat
Hacktivism	■ To invade web pages and computers to create pressure	■ Hack by malware ■ Hack by ransomware ■ Credential theft ■ Privacy violation
Cyber criminality	■ To gain financial benefits ■ To inflict personally motivated harm	■ Revenge or bullying ■ Criminal damage ■ Robbery of cargo ■ Identity theft ■ Data breach ■ Data damage ■ Illicit gambling or spreading false information ■ Copyright or brand violation
Cyber espionage	■ To gain competitive advantage and intellectual property of other business ■ To interrupt business operations ■ To damage company reputation	■ Illegal access to secret and delicate information such as company strategy, private information or intellectual capital ■ Cyber extortion ■ Information stealing ■ Insiders gaining unauthorized access to information systems ■ Intruder having direct physical access to systems and the network ■ Cross contamination ■ Cyber fraud
Cyber terrorism	■ To politically attack information, computer systems, computer software and databases	■ Outage and information system failure ■ Website defacement ■ Subversion of security control Sabotage
Cyber war	■ To fight against opponent countries by damaging or disabling their rivals' computer networks, especially relevant to military affairs	■ Sabotage at national level ■ Disruptive attacks by state actors

Higiene da Cibersegurança Portuária

- Humana
  - Treinamento da força de trabalho
  - Conscientização sobre segurança da força de trabalho
  - Treinamento de executivos
  - Conscientização de segurança dos executivos
  - Equipe de segurança de TI e equipe de resposta
  - Cultura de segurança dos trabalhadores

Higiene da Cibersegurança Portuária

- Infra-Estrutura
  - Infraestrutura física e commodities
    - Edifício de escritórios
    - Centro de operações do terminal
    - Carga

Higiene da Cibersegurança Portuária

- Infra-Estrutura
  - Veículos e equipamentos
    - Embarcações e camiões de longo curso
    - Equipamentos para movimentação de cargas
    - Equipamentos e veículos automatizados para movimentação de cargas
    - Equipamento de apoio à navegação
    - Ferramentas de depósito vazias
    - Ferramentas e-Desk
    - Dispositivos de Internet das Coisas (por exemplo, sensores e câmera)
    - Outras máquinas e equipamentos

Higiene da Cibersegurança Portuária

- Infra-Estrutura
  - Sistema de operação e controle portuário
    - Sistema de controle de acesso à porta
    - Sistema terrestre para operação e navegação de embarcações
    - Sistema automatizado de rastreamento de contêineres de carga
    - Sistema de controle de uso da Internet
    - Sistema de controle de manuseio
    - Sistema de controle de tráfego
    - Sistema de controle predial
    - Sistema de controle de acesso ao armazém
    - Rede interna de trabalho
    - Rede de colaboração empresarial externa
    - Tecnologia da informação aduaneira

Higiene da Cibersegurança Portuária

- Infra-Estrutura
  - Infraestrutura de informações para apoiar a segurança cibernética portuária
    - Segurança da informação
    - Segurança de aplicativos
    - Proteção contra ameaças cibernéticas
    - Segurança na Internet
    - Segurança de rede

Higiene da Cibersegurança Portuária

- Procedimento
  - Gestão de riscos
  - Governança de risco portuário
  - Gestão de mudanças
  - Compartilhamento de informações
  - Gerenciamento de ameaças e vulnerabilidades
  - Resposta a eventos e incidentes
  - Gestão cibernética e de programas
  - Medida de resiliência e redundância do sistema
  - Gestão de danos
  - ISO 31000:2009 e ISO/IEC 27005:2011

Precisando, me contate:

Bruno Eduardo Budal Lobo
048 99998-2777

Instagram:
bruno.blobo
LinkedIn:
brunoblobo

bruno@loboevaz.com.br

Lobo & Vaz Advogados Associados
www.loboevaz.com.br