FUSION Computing
416-566-2845
www.FusionComputing.ca

TRANSPORT & LOGISTICS

Although digital transformation and automation of the transport and logistics sector are proving to be a boon, they have also made the industry an easy and sought-after target for cybercrime. As most or all levels of the supply chain are rapidly integrated with the cloud, significant cybersecurity risks have emerged. This sector is particularly vulnerable to cyber-related incidents with many stakeholders and third-party vendors in the logistics chain.

Some Key Areas To Review:

PHISHING

Logistics and shipping companies are increasingly being targeted by phishing attacks.

Cybercriminals contact users and impersonate legitimate business contacts.

Targets are lured into giving up sensitive data and access to company resources.

RANSOMWARE

It locks down systems and prevents access until a ransom is paid.

It is one of the fastest-growing types of cybercrime.

SUPPLY CHAIN ATTACKS

Threat actors access an organization's network via a third-party vendor or supplier.

In recent years, supply chain attacks within the manufacturing industry have become more prominent.

It can take the form of hardware, software and firmware-based supply chain attacks.

In May 2021, the Colonial Ppolhe attack disrupted jet fuel and gasoline supplies to large areas of the southeastern region of the U.S. While the direct financial Impact was the payment of a $4.4 million ransom, the Indirect financial and socioeconomic Impacts to the associated supply chain were far greater. The crippling attack cost the company $40 million in charges on lost shipping opportunities and a further $20 million in investigation, recovery and remediation expenses.

INDUSTRIAL IOT ATTACKS

Industrial IoT (Internet of Things) devices like printers and smart TVs are at a high risk of attack.

Each device should have a strong, unique ID and up-to-date software. Unnecessary services and ports must be disabled.

Devices utilizing manufacturing processes, such as Remote Production and Industrial Asset Management, are at risk.

Network activity must be monitored to determine unauthorized use.

PRIVILEGED ACCESS MANAGEMENT

Any account that provides access and privileges beyond those of non-privileged accounts.

Privileged users/privileged accounts pose considerably larger risks.

Implement Privileged Access Management (PAM) solutions to secure accounts and users.

FUSION Computing

TRANSPORT & LOGISTICS

Key NIST/CyberSecure Canada control points:

VULNERABILITY MANAGEMENT

It is important to update devices and software on a regular basis.

Ensures devices and applications are protected from attacks and operating efficiently.

Restricting unauthorized software applications can help mitigate exposure to potential attacks.

NETWORK SEGMENTATION & CENTRALIZED MANAGEMENT

Network segmentation and Zero Trust are key areas of a secured network layer.

Segment network, limiting impact in case of an attack.

Centralized management must establish controls to protect the expanding lot attack surface.

Stronger encryption mechanisms and identity authentication protocols to be implemented.

MULTI-LAYERED IT SECURITY

All systems should have regular security updates.

Network design strategies must be implemented with proper zoning and micro-segmentation.

Use of firewalls, antivirus and EDR solutions and more.

Security awareness training for all employees teaches users to look out for threats and flag them

CONTINUOUS MONITORING

An ongoing process to spot vulnerabilities and threats to order to support organizational risk management.

The NIST framework provides a clear roadmap for compliance and continuous improvement.

Protect reputational and financial damage, loss of competitive advantage, and potentially increase generated revenues.

FUSION COMPUTING targeted remediation:

RISK ASSESSMENTS

Risk must be gauged based on factors such as probability of occurrence, impact on the organization, and risk prioritization.

Risk assessments should be conducted or reviewed regularly and at least once per year.

SECURITY CONTROLS

- Anti-virus and MDR
- Secure encrypted backups
- Data Loss Prevention
- Encryption at rest and in transit
- Firewall
- Incident Response Plan
- Mobile Device Management
- Policies and procedures
- Security Awareness Training
- Vulnerability Management
- Multi-Factor Authentication

CIS Controls