HDI Risk Consulting

Cybersecurity in the logistics sector

www.hdi.global

FACT SHEET

Cybersecurity in the logistics sector.

Transport and logistics are becoming increasingly dependent on digital information. Important systems such as Warehouse Management Software (WMS), Transport Management Software (TMS) and Fleet Management Software (FMS) are important tools for logistics service providers. But also links with mobile devices or on-board computers in trucks play an increasingly important role. Through automation in logistics, a lot of time can be saved and processes can be continuously optimised.

This high level of automation also entails risks. The unavailability of this type of systems due to ransomware, DDoS attacks or the manipulation of digital information can cause extensive damage to logistics service providers. The availability, integrity and confidentiality of information and systems can be compromised.

Threats

Awareness of digital threats and their consequences for the organisation is extremely important to prevent cyber incidents. A system that is not available due to ransomware can have major consequences including the planning, order processing or availability of goods in a warehouse. In the worst case, the ransomware can cause an entire truck fleet to come to a complete standstill. It can take a long time before an affected system is repaired. There is also a high risk of data being lost, such as orders placed, invoices or planning data. This can result in subsequent reputational damage because invoices are not paid or ordered goods are not delivered. And who can be sure that the ransomware has been removed completely after the system has been restored?

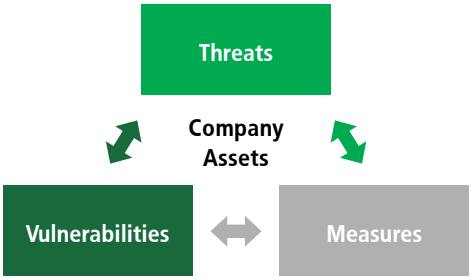
Another increasingly common threat is the manipulation of bills of lading by cyber criminals. They can gain access to logistics systems through the back door. They then use this to find delivery addresses or PIN codes for the pick-up of containers as an example. Many other kinds of cybercrimes are possible, for example:

- Phishing emails
- CEO-fraud
- Social engineering
- DDoS attacks
- GPS jamming

The human factor plays an important role in cyber incidents as most incidents are caused by human unawareness. Think of phishing emails with a malicious link. After clicking on this link, malicious software (malware) is installed. It is also possible that emails ask for the username and password for an important system.

Measures

The board, management and employees of logistics organisations must therefore be very aware of the threats and vulnerabilities of their digital systems. Take appropriate measures to remove them as much as possible.



It is necessary to identify all the critical resources a company has to offer. Think of data, software and hardware as well as employees, procedures, policies and suppliers.

Determine what the threats are by any means, such as systems that are no longer available due to ransomware or fake emails from CEOs asking for large sums of money to be transferred.

Determine what the vulnerabilities of these resources are. For example, employees who are not sufficiently aware of the rules for information security, data streams that are not en-crypted or software that has not been updated or has not been updated on time.

Finally, take appropriate measures to eliminate the identified vulnerabilities and threats as much as possible:

- Organisational: Drawing up an information security policy of high quality or providing in-formation and ICT awareness training to your employees.
- Technical: Well-equipped firewalls, antivirus software, encrypting data or shutting down USB ports.
- Physical: Closing server rooms, using camera systems and/or motion sensors and, for example, physically limiting networks.

Priority

The dependence on digital systems in the logistics sector has increased enormously. The downside of this is that digital threats and vulnerabilities have increased and can do a lot of damage to your organisation. Be prepared to reduce these threats and vulnerabilities as much as possible. Make information and ICT security the highest possible priority.

Contact

For questions and/or more information you can contact us via:
HDI Risk Consulting
T: +31 (0)10 – 40 36 328
hrc@nl.hdi.global
www.hrc-services.nl

Benefits of HDI Risk Consulting

- HDI Risk Consulting Professionals offer risk and safety related analysis to enable specific risk prevention action plans to be developed.
- Qualified international Risk Engineering network offers clients worldwide multi-discipline support in Risk Engineering.
- HDI Risk Consulting is a wholly owned subsidiary of HDI Global SE and thus part of the Talanx Group, one of the largest insurance groups in Germany and Europe.

403-HRC244GB 201907