EU MONITORING
EPTDA
Volume 4-2019

Cyber-attacks in Logistics

July 2019

New technologies can bring many opportunities for organizations, but they also offer cyber criminals many ways to harm your business, deceive your customers, and spoil your reputation.

That is why is important to know that investing in preventing and tackling s is mandatory for any company, especially for EPTDA members: the logistics sector is an important target for hackers because it manages a huge and diverse amount of data.

Types of Cyber-attacks

Cyber-attacks are divided into five main categories:

1. **Data breach:** Release of secure information to an untrusted environment, including trade data, schematics, manufacturing systems, shipping data, and other confidential company information.
2. **Ransomware**: A form of malware which encrypts a user or end system, rendering all data within inaccessible, and demanding the payment of ransom to decrypt.
3. **Denial of Service (DoS):** Performed by many actors to render a firm's website or system unavailable to users.
4. **Vulnerability:** The discovery of a weakness, known or unknown, which may be exploited by a threat actor to perform unauthorized actions on a system.
5. **Phishing:** A fraudulent attempt to obtain security credentials from entry to executive levels for malicious purposes.

Each category contains several subcategories, but these are the most important computer threats that companies may face.

The economic impact of cybercrime has increased fivefold between 2013 and 2017, affecting both governments and businesses. The expected increase in premiums cyber insurance, from € 3 billion in 2018 to € 8.9 billion in 2020, also reflects this trend.[1]

Stages of a Cyber-attack

First, a malicious actor will start by collecting information on a specific organization or company, such as schematics, business emails, and the source code for internal applications, among others.

Once information is collected, the next step is to assemble the virus, bug, or malware. Then, the attack is sent to the target organization, which could be in the form of a phishing email, a hardware or software vulnerability unknown to the user or manufacturer, or a brute force entry through a network weak point.

Afterwards, hackers look for ways to gain more control by identifying and impersonating accounts that have management privileges, which gives them deeper access to the systems.

Once an attacker has widespread access to the network, they will infiltrate as many systems as possible. They may look to establish means for long-term access while evading detection using malware "implants" installed without your knowledge.

Some hackers just want to get in, get something, and get out—in other words, a smash-and-grab approach. But others decide to stay a while using longer-term hacking techniques.

Cyber-attacks: by the numbers

Although 80% of EU businesses have experienced at least one cyber-security incident in 2016, the awareness continues to be alarmingly low[2]. 69% of EU businesses do not understand the potential impact of a cyber-attack or have a vague idea about it, and 60% did not estimate the potential financial losses not even once (costs could include: revenue loss, system repair costs impaired, possible financial liabilities for assets or stolen information, incentives necessary to keep customers, higher insurance premiums, protection costs, potential agreements on compliance costs or litigation).

In addition, one-third of organizations would prefer to pay the ransom requested by a hacker rather than investing in cyber-protection, according to a global study.[3]

In 2017, cyber-crime costs accelerated with organizations spending nearly 23 percent more than 2016 — on average about € 11.2 million.[4]

It is also important to mention that nearly half of the security risk that organizations face stems from having multiple security vendors and products.[5]

Alarmingly, it takes organizations an average of 191 days to identify data breaches.[6]

2017: A tipping point for supply chain Cyber-attacks

2017 was declared a "watershed" year in terms of cyber-attacks, with an increase of 400% since the previous year. Many of them were made through supply chain infiltration.

In 2017, there were seven cyber-attacks targeting the supply chain. By comparison, only four such incidents had been reported between 2014 and 2016.

The most famous of them was WannaCry, which caused a multi-continental ransomware lockout that cost a single shipping line over $ 300 million.

Another example is the Netsarang security breach, which allowed hackers to steal valuable information from companies across sectors, including transportation. In this case, they used a tainted version of CCleaner – a PC cleanup tool – and obtained control over hundreds of thousands of computers.

Another notorious targeting a supply chain system was NotPetya. In this case, hackers hijacked updates for a piece of Ukrainian accounting software in order to inject a destructive worm which caused losses of $ 10 million worldwide.

Of the cyber-attacks identified in 2017, 1 out of 13 were malware. Of these, 93% were related to the latest versions of different kind of software, indicating an escalation of computer threats. Also, overall vulnerabilities have increased by 13%, while there has been a 29% increase in vulnerabilities within Industrial Control Systems (ICSs).

Impacts of Cyber-attacks

Operational impacts:

- Daily operations are slowed down or blocked; in the last case, this could severely disable the production lines; if the blockage lasts for more than a day, then costs could reach hundreds of millions of dollars.
- The loss of real capital, such as intellectual property or data crucial to the organizations' functions that will have an immediate and tangible loss.
- The loss of communication: the company could not reach its clients or its partners.
- The loss of supply chain control, where through breaches at suppliers and transportation hubs, organizations are unable to perform normal operations, and thus lose revenue.

Reputational impacts:

- If the attack information gets out, then the company can become a target for further attacks, it can lose the trust of its clients, thus affecting its future plans; a PwC survey of British firms in 2015 revealed that of firms reporting a damage to reputation, 57% of the damage was due to media coverage and customer complaints.

Legal impacts:

- The General Data Protection Regulation (GDPR) states that any entity that was affected by a data breach of any sort should inform the authorities and any other party that could have been affected within 72 hours of the discovery of the attack; otherwise, that entity could be fined with maximum EUR 20 million for non-compliance with the European legislation.

Cyber-attacks in logistics: Challenges and solutions

Data security is crucial for all organizations. Information about consumers such as their payments, personal records, banking account details – all these are often impossible to replace if they are lost and they become dangerous if they get into the hands of criminals.

Data loss caused by disasters such as flooding or fire is devastating, but if they came into hacker's hand or are contaminated by malicious software, it may have far greater consequences. How you handle and protect your data is essential to your business.

Given the amount of information they handle, logistics companies are a more appealing target for hackers.

In order to prevent and manage cyber-related risks, it is recommended to have a response plan that includes the implementation of control processes in terms of risks for early detection of threats:

1. **Risk identification:** Determine which suppliers or third parties may have access to your firewall, and which one would have the greatest impact on your organization in the event of a cyber-attack. Also, when selecting your suppliers, you should perform a cyber-security analysis and identify what kind of data you send to them. Afterwards, you need to determine what steps you need to take in order to ensure data protection.

2. **Incident monitoring:** As cyber threats become more sophisticated, your business needs to make a continuous effort in order to improve the evaluation and understanding of events that affect suppliers or third parties that work with you. This will become crucial when you will be attacked by hackers.

3. **Evaluate potential effects:** Organizations should be aware of the impact that a cyber-attack may have on the business. Therefore, it is recommended that organizations assess all vulnerabilities, from multiple angles, in order to determine what the easiest way to attack could be. By understanding this aspect, you will be able to prevent an attack, or you will be better prepared to respond effectively in the aftermath of a cyber-attack. By doing this, you could protect the supply chain.

4. **Develop risk scenarios:** This will help you plan the response methods for various situations that may arise, equip you appropriately, and establish clear protocols. You also need to prepare your emergency response team to know what to do in the event of a cyber-attack.

5. **Response actions:** Once a cyber-threat has been identified, it is mandatory to investigate the matter and pass on the relevant information about the attack to the authorities. Once it is 100% confirmed, organizations should be proactive and announce their stakeholders and partners and then keep them informed about the solutions they have adopted.

In addition to having a response plan in place, companies should follow three overarching principles that can best prepare them for potential vulnerabilities in the supply chains in the context of cyber-space:

a) Accepting the inevitability of an attack,
b) Ensuring continuous monitoring, and
c) Communicating across one's supply chain to ensure a consistent standard.

Here are some practical examples that EPTDA members can adopt in order to strengthen the cyber-security of their organization (via DHL Resilience360 Special Report, published in 2018):

- **Protection and encryption of remotely stored data:** Protecting remotely stored data will greatly reduce the risk of sensitive material being compromised in the event of a breach, and if encrypted, will provide even further protection beyond the scope of what is within one's power. This is especially necessary when organizations share data with their suppliers.
- **Segmenting your networks:** By ensuring a common understanding of segmentation in your organization and in that of your suppliers, risks can be significantly diminished.
- **Thorough audit of suppliers and planning for accidental or intentional manipulation:** Development of custom software and network configurations when possible to account for accidental or intentional manipulation or disclosure. Conducting these exercises with suppliers can ensure readiness in the face of an uncertain cyber threat environment.
- **Preparation of multiple backup options:** The establishment of backup means of communication and operation through a formalized continuity plan can make all the difference in operations mid-breach; even more preferable would be a contingency employing internal and non-open source tools.

You should not forget that people are the primary vulnerability. Therefore, you need to train them so that they understand the risks of a cyber-attack.

Social engineering, also known as "pretexting", is used by many cyber-criminals to deceive and convince the target to provide, often unknowingly, the information they need and / or install a malicious software on computers, devices or networks. Social engineering is successful because attackers do everything, they can for their work to look and sound legitimate or even useful.

Social engineering can also take place over the phone, but it usually happens frequently online. The information gathered from social networks or displayed on certain websites can be enough to create a convincing ruse. For example, LinkedIn profiles, posts on Facebook and Twitter posts could allow an attacker to obtain detailed records about employees. Staff training on the risks involved in publishing personal or business details over the Internet is a useful tool for prevention.

Many cyber criminals use social engineering tactics to convince users to voluntarily install malicious software on computers, such as false antivirus, believing that they are doing something helpful. In this way, an attacker could take the control over a device or a system and steal sensitive information, for example. Malicious software can also make system changes that could became dangerous. It is important to not click on pop-ups that display questionable warnings. Also, people should not provide credit card information without a proper verification of the website in advance.

It is also helpful to keep a constant online messaging with your customers and business partners in order to prevent others from impersonating someone from your organization. It is recommended to not require personal information or account details by email, social networks or other online messages. Employee awareness is the best defense against hackers!

Explain to everyone that they should not respond to the incoming messages requesting information personal. If an outside entity claims to be a legal organization, check the information before. Also, employees should know to never click on a link that came from an unreliable source.

If you think you have revealed sensitive information about organization, make sure that:

- You report this to those responsible within the organization
- You contact your bank and close any accounts compromised (if you believe financial data is at risk)
- You change any passwords you have revealed and if you used the same password for more resources, make sure you change it for each account.

Also, if possible, configure your computers so you do not allow all users to have administrative access. This will minimize the risk that they will install malicious software and compromise the entire organization.

In conclusion, combining methods like web filtering, having an antivirus, proactive protection against malicious software, installing and updating firewalls, keeping your software up to date, having a robust cybersecurity policies and training your employees regarding cyber-security risks, you significantly reduce the possibility of becoming a victim.

EU Cybersecurity Act

The EU Cybersecurity Act revamps and strengthens the EU Agency for cybersecurity (ENISA) and establishes an EU-wide cybersecurity certification framework for digital products, services and processes.

In particular, ENISA will have a key role in setting up and maintaining the European cybersecurity certification framework by preparing the technical ground for specific certification schemes and informing the public on the certification schemes as well as the issued certificates through a dedicated website – www.enisa.europa.eu/about-enisa - according to the European Commission.

ENISA is also mandated to increase operational cooperation at EU level, helping EU Member States who would request it to handle cybersecurity incidents, and supporting the coordination of the EU in case of large-scale cross borders s and crises. This task builds on ENISA's role as secretariat of the national Computer Security Incidents Response Teams (CSIRTs) Network, established by the Directive on security of network and information systems (NIS Directive).

On the other hand, the EU Cybersecurity Act introduces for the first time an EU-wide cybersecurity certification framework for ICT products, services and processes. Companies doing business in the EU will benefit from having to certify their ICT products, processes and services only once and see their certificates recognized across the European Union. More on the Cybersecurity Act.

The NIS Directive creates a good framework for network and information security at national level for each EU Member State. The most important part that regards companies directly refers to "essential service providers", which must:

- Take appropriate technical and organizational measures to address the risks regarding their security of the networks and computer systems
- Take appropriate measures to prevent and minimize the impact of the incidents affecting the security of their networks and computer systems
- Notify the competent authority of the incidents that have a significant impact on the continuity of the essential services they provide

Another important aspect of security for the EU is data protection covered by the General Data Protection Regulation (GDPR).

Critical Sources and further reading:

- Cerasis, Cybersecurity in the Supply Chain: Challenges and Solutions as the Supply Chain Goes Digital
- Biologitik, Cybersecurity challenges in logistics and transport
- More than Shipping, The Importance of Cybersecurity in Logistics
- European Commission, Cybersecurity Act 2018
- DHL, Resilience 360 Report

Notes:

[1]European Commission, State of the Union 2017 - Cybersecurity: Commission scales up EU's response to cyber-attacks

[2]Europol, Internet Organized Crime Threat Assessment 2017

[3]NTT Security, Risk: Value 2018 Report

[4]Accenture Report

[5]Cisco Report

[6]CSOonline, Top Cybersecurity facts, figures and statistics for 2018