PORT CYBER SECURITY

A CHALLENGE FOR EVERY LINK IN THE SUPPLY CHAIN

Catalina Grimalt, Deputy manager of Organisation and Internal Resources, Port de Barcelona

Cyber security is a growing concern for companies in the light of the large-scale digitalization process that they have experienced and continue to undergo. These rapid transformation processes have brought about major technological advances and improvements, but they have also given rise to new problems that must be addressed: cyber-attacks.

The technological environment that is a feature of modern ports entails a heightened risk from cyber threats, making greater protection essential. Cyber criminals can attack from multiple points of entry and, moreover, the interdependence of systems and electronic devices, the relative ease with which successful attacks can be made and the profit derived from them, along with the difficulty of identifying the culprits, lead to a rise in attacks of this kind. Security must be boosted in parallel with the increase in the digital services on offer.

THE PORT OF BARCELONA

The Port of Barcelona, in addition to the usual protection and defence measures taken by any company, has had a cyber security plan in operation for a number of years that focuses on various aspects: adapting legislation, developing specific policies, simulating attacks and training employees, among others.

An important infrastructure like a port is subject to daily attacks, consisting of vulnerability scans of its public IPs. However, the truly worrying attacks are the ones that cannot be seen. For this reason, the Port of Barcelona constantly performs a wide range of monitoring activities in collaboration with a number of public and private bodies to provide an optimal service.

As a result of all these changes, we have been able to put a cyber security plan in place that is aligned with the global strategy of the port, improve security in computer systems and applications, provide cyber security support for new developments, raise employee awareness, constantly manage security, preventively and reactively, and apply clearly defined security policies.

THE ROLE OF PORTS IN THE SUPPLY CHAIN

In addition, the role of ports in the supply chain is to be the point of origin or destination of goods. The remaining processes in the chain are undertaken by other companies. For this reason, any disruption or problem in the chain affects both the end customer and many other companies.

The Port Authority is just one more link in the supply chain. As such, the Port of Barcelona has already begun to work on contingency and resilience plans in conjunction with the companies that operate in the port or whose activity is associated with the port territory. In this regard, it is essential to share information to minimise the impact on the supply chain.

COORDINATION AMONG COMPANIES THAT OPERATE IN THE PORT

Coordination structures are in place to share information by using other technological forums. As an ambition for the years ahead, the Port of Barcelona intends to establish a coordinated connection space to give a unified response to any threats that unfold.

In the past, the movement of goods was virtually independent of the movement of information. Today, most companies rely heavily on processes that can only be performed by using technology. For example, terminal or warehouse movements, which in many cases are now highly automated; documentation processes with public administrations that can only be completed electronically or documentation processes between companies to move goods in ports, which are based on the information available in the port community systems'.

In this scenario, it is essential to coordinate all the companies that operate in the port in a number of respects. Firstly, so that the various companies are able to share, quickly and effectively, a number of good cyber security practices. Secondly, to share early warnings for incidents that may occur in businesses in the community. Finally, to draw up response plans for joint incidents to minimise the possible impact of an incident on the operation of the chain.

NEW CHALLENGES

The complexity of the situation gives rise to highly varied new challenges. One of the most important is ending the shortage of trained and reliable engineers who are able to work in cyber security. Another challenge concerns the control mechanisms of a public company and the changes that occur as regards technologies. Consolidating these challenges is one of the main risk factors that must be addressed daily. Finally, awareness by company employees of the importance of cyber security and the major role that their actions play in facilitating the work of some cyber criminals is crucial to avoid certain attacks.

It must be understood that this requires a change of mentality for the whole company and that is a truly profound change. In this context, the awareness and training of port workers is crucial. It is also important to bear in mind that it is impossible to achieve absolute security. As such, it is necessary to have protocols in place for each known type of cyber attack.

Finally, the main technological challenge, given the large number of possible solutions and options, is finding the response that can offer the greatest value to our companies at the best possible cost and implementing it as a priority. In addition, these measures must be introduced at every level: from each employee's post, to applications, their development and the use made of the applications by users.

ABOUT THE AUTHOR

Catalina Grimalt, Deputy manager of Organisation and Internal Resources at Port de Barcelona.

ABOUT THE ORGANIZATION

The Port of Barcelona is the fastest-growing port in Western Europe and it is part of a unique and seamless logistics and business hub, including airport, port, logistics areas and a large urban area. It is Spain's top port for international trade.