Port agents get access to the cloud

Girija Shettar, Senior Editor | 4 April 2016

Port congestion might be relieved with cloud computing for port agents. Credit: Dietmar Hasenpusch.

A maritime technology company, that has created and launched a cloud-based system for port agents, claims it will improve security and efficiencies at ports for ship charterers and owners.

The Softship system, known as Softship Advanced Port Agency Solution (SAPAS), has been formulated to create a checklist of all the critical services a port agent has to provide to a ship, creating, said the company, a “checklist, statement of facts and a disbursement account that can be presented when the vessel departs”.

Speaking to *IHS Fairplay*, group marketing manager, Lars Fischer, said the system could avoid costly mistakes that occur currently with the manual processing of data via the use of non-proprietary products such as Microsoft Excel or Word.

“A small delay during a port call could end in a major expense for the charterer or owner. If, for example, a port agent forgets to submit licences or certifications, the ship might not be allowed into the port.”

The cloud-based system does not require investment in software, hardware, or services, is pay as you go requiring no ongoing subscription fee, and is accessible from anywhere via mobiles and tablets.

The system will handle potentially sensitive data, such as ship ETAs, vessel types, and cargoes. Fischer said, however, that security of data stored on the cloud system is likely to be higher than if it were stored directly on the hard drive of a port agent's device.

There is in place a three-step security barrier, Fischer explained, which begins with ensuring a secure connection between the user and the system, known as 'front-end' security. This involves an authorisation process wherein the user must identify him or herself through their credentials.

The second layer of security is that all data goes through a secured, https, connection, which means that all the data that travels between the user and the server is encrypted and unreadable.

"We have a secured, encrypted, connection between your device to the server. This is important – there is no local installation on your device; no piece of software is installed. The data goes purely through the web," said Fischer.

The third layer of security is at the data storage centre – in this case at the Softship facility in Hamburg, Germany. This, said Fischer, is secured through "various mechanisms and means to ensure that it will not be able to be hacked through professional hackers".

In terms of data protection laws, the system is much like any other, for example when using Apple products or a banking system: terms and conditions of the system are visible to the user on signing up to the platform, which the user must confirm acceptance of every time a transaction is processed.

One key cloud computing concern is that data in the cloud is, in effect, in the public domain and should security fail, that data will be publicly available – technically known as 'isolation failure'.

However, Fischer said that he sees the cloud as potentially more secure, "People think that if they have everything in their own office on their own devices everything is safe and secure. This is not the case, because they are connected to the internet and the problem with these open networks is that they can be pretty insecure if you do not use the latest technology.

"But we as a cloud service provider have to use the latest technologies, otherwise we are unable to provide a secure and safe service.

“So, in the end it could be more secure to put your data into the public domain, the cloud, rather than keeping it in your own office,” he said.

Advice to users from official sources includes checks on: ensuring there is a privacy agreement and service legal agreement; the location of where the data is to be stored, because it is the laws in this jurisdiction that will bear upon that data; and how data will be stored and secured. And if storing personal data, the user should be aware of his/her/others' legislative and regulatory requirements.

One of the most downloaded documents from the European Network and Information Security Agency is: *Cloud Computing: benefits, risks and recommendations for information security (2009)* http://bit.ly/1N4Q6nc. This recommends that standard contract clauses may deserve additional review because of the nature of cloud computing.

"The parties to a contract should pay particular attention to their rights and obligations related to notifications of breaches in security, data transfers, creation of derivative works, change of control, and access to data by law-enforcement entities.

"Because the cloud can be used to outsource critical internal infrastructure, and the interruption of that infrastructure may have wide-ranging effects, the parties should carefully consider whether standard limitations on liability adequately represent allocations of liability, given the parties’ use of the cloud, or responsibilities for infrastructure," states the document.