Sector Focus: Public Transport

Published 27 July 2021

Following on from our focus on the food manufacturing and education sectors, an additional sector which has recently fallen victim to the increasing wave of cyber attacks is the public transport sector which is a provider of critical infrastructure. The sector tends to be heavily dependent on efficient computer networks and technology to manage business, therefore making companies ripe targets for a cyber attack.

Transportation companies also present a tempting target as there tend to be multiple opportunities to infiltrate their networks thanks to the interconnected nature of the business. Threat actors can find a weak link within the vast network and then use that to gain entry and spread ransomware throughout the entire system. Additionally, although the transport and logistics sector is recognised as one of the largest and most profitable industries worldwide, relatively low investment has generally been made in to cybersecurity infrastructure.

A recent attack targeted at the public transport sector occurred on 9 July 2021 when Iran's state railway system fell victim to a cyber attack. Whilst an initial report cited "unprecedented chaos" was subsequently deleted, it has been reported that the attack led to cancellations and delays on hundreds of lines as departure notice boards were manipulated to warn of delays due to a cyberattack. Departure boards inside some train stations also listed the phone number for the office of the supreme leader, Ayatollah Ali Kamenei, and encouraged passengers to call his number for more information. Shortly after the potential attack, Iran's telecoms minister, Mohammad Javad Azari, warned about possible cyber attacks via ransomware.

In addition to the impact on a company's infrastructure, this can also give rise to concerns about passenger safety. Such concerns were raised when the New York City subway authority, Metropolitan Transit Authority (**"MTA"**), was hacked in April 2021. The MTA is North America's largest transportation network with over 15.3 million users around New York City. Fortunately, the threat actor was unable to access MTA's systems which controlled the train cars. Nonetheless, this incident demonstrates the potential for passenger safety to be impacted by future cyber-attacks on the public transport sector. Moreover, passenger complaints are likely to follow due to the delays to transport. Nottingham City Transport (**"NCT"**) was recently faced with a cyber incident in which it warned that passengers may face "*intermittent disruption as the systems which are used as part of [its] operation are currently unavailable*". Fortunately, NCT was able to continue its bus services with a slight disruption.

In other cases, public transport entities have had to take systems offline for longer periods of time. Northern rail, which is run by the UK government, recently announced that its self-service ticket machines had to be taken offline for a period of at least a week whilst investigations were under way following a suspected ransomware cyber attack. Ultimately, the operational consequences of a cyber attack on the transport sector are highly visible and affect many.

Given the widespread reliance on public transportation companies, any companies who fall victim to a cyber attack are under pressure to quickly restore operations. Much tends to be lost in sales following a cyber incident, in addition to the costs spent on IT support, forensic investigations and breach counsel support. The disruption to staff productivity is also a concern for this sector.

Public transport companies also hold vast amounts of personal data on their customers and employees. This includes data such as financial information, contact information, health data, etc. Therefore, there is also the risk that a cyber attack could be used to exfiltrate personal data and encrypt a company's system, to force the hand of public transport companies to pay a ransom in order to restore business and prevent the sale of personal data.

Public entities that provide an important role in the transport sector are also likely to be defined as an operator of essential service under the Security of Network & Information Systems Regulations (**"NIS Directive"**). Under the Directive, identified operators of essential services have to notify serious cyber incidents to their competent authority. This means that following a cyber attack, a public transport company who is an operator of essential services will need to consider its notification requirements under the NIS Directive. This is in addition to its notification requirements under the GDPR.

As a result of the constant threat of cyber attacks on the transport sector, we would advise all providers to have in place a robust breach management plan and cyber insurance policy in order to cover the costs of such incidents. With the rise in cybersecurity incidents in the transport sector, the chances of being a target is a very real and immediate risk for all.

Authors

DAC BEACHCROFT