KCS Group Europe

Travelex hack: the road to nowhere…

16th January 2020

A few years ago, the German and Russian secret services invested in typewriters, to ensure that their communications could not be intercepted by foreign powers and to enable them to continue their work in the event of a cyber compromise. Currently, the travel money provider Travelex must be wishing it invested in typewriters – or rather, better cyber defences. The firm was forced to use pen and paper after seeing its entire cyber capacity hamstrung by a ransomware attack, which illustrates that as we enter a new decade, the threats to IT well-being are as prevalent as ever.

Travelex was hit by the Sodinokibi ransomware – a relatively standard tool encrypting all files and asking for Bitcoin for their release – and faced the sale of significant quantities of personal customer data unless it payed £3m GBP in ransom. Of course, as with all ransomware, there is zero guarantee that data will be restored, but this was rather beside the point. The reputational damage to Travelex has already been done, given the embarrassment of a very public and large-scale compromise, ongoing financial damage (with shares in its parent company plummeting to a record low), and customer (not to say investor) confidence surely badly hit.

While the company is by no means alone in falling prey to ransomware hackers, the public scale of the response – the total move to pen-and-paper and the difficulty this caused in the maintenance of business – highlights how damaging the fallout can be from just one successful bad action. For a cyber-reliant company, it is disastrous. For a critical industry company, it would be fatal.

Not only does this illustrate just how easy it can be to essentially bring a company to its knees, but the degree to which the various elements of cyber-criminality feed off each other and which gives the lie to the idea that businesses have nothing worth stealing, or that they are unlikely to be a target. Stealing the Travelex data purely for a financial ransom is one thing, even working on the basis that few and far between are the firms that pay up. However, having the vastness of the marketplaces on the Dark Web means the bad actors have a backup if their Plan A does not work out – and it is one that is a good deal more lucrative, if they are able to sell on the data (and any weaknesses they may have identified in the target company, such as compromised passwords) multiple times on the dark web, the threat profile is thus greatly increased as well.

This Travelex incident is emblematic of 'the worst' that can occur in the world when business is more reliant on technology than ever – unavoidable – but also of how the impact footprint is ever-widening. As well as the already identified concern about hackers having the entirety of the dark web to sell their spoils, and the ripples widening out from the immediate impact of the loss of competencies, others down the supply chain are suffering as well – not least banks such as RBS, Lloyds and HSBC, all of which saw their online travel money capabilities down as a result of the initial compromise. And of course, it can never be ruled out that the initial target is but a means to an end to reach another, more valuable objective.

It is a new year, but the same threats remain!