To pay or not to pay?

Flavia Kenyon outlines the increasing threat of ransomware cyber attacks on big business

Ransomware—to pay or not to pay—this is the drama facing multinational foreign currency company Travelex at the beginning of 2020. The company's office in London has fallen victim to a ransomware cyber attack paralysing its entire network and causing the company to take down its websites worldwide.

Ransomware attacks are on the increase worldwide, with a worrying resurgence in the last two years. Variants such as Sodinokibi, the malware used in the attack on Travelex, have caused havoc for businesses and government agencies globally in targeted ransomware attacks intent upon extorting millions of pounds/dollars/the bitcoin equivalent. In this case the attackers have demanded £2.3m to allow the company back into its own systems. It is still unclear how those negotiations are being played out.

Sodinokibi seems to be the current malware of choice. It was used in previous attacks by imitating Booking.com, a legitimate hotel booking service in order to entice users to open a malicious email or link.

By the end of 2019, such was the level of sophistication of ransomware, that cyber security analysts began referring to it with terms normally used for legitimate business models; a 'service market', a big business market, a 'big game hunting' market for criminal groups run as professional organisations.

The attackers use research to select targets based upon their vulnerability from small/medium businesses to large/global businesses, such as Travelex. They work as an organised criminal enterprise with groups/branches performing different functions: one group might specialise in obtaining RDP (remote desktop protocol) access to a compromised network/device. This is often bought off the shelf from RDP 'shops' on the dark web. RDP access has become a hot commodity. Once access is obtained it is passed on to another group who specialise in building the platform and installing the ransomware. Criminals often partner with software developers for a percentage of the ransom money.

There has also been an increase in attacks targeting the critical infrastructure of big cities. In July 2019 City Power, the major electricity provider in Johannesburg, South Africa, was hit, affecting hundreds of thousands of people and businesses. Also in 2019, in the State of Texas 22 government agencies were targeted in a highly sophisticated and choreographed ransomware attack. In the State of Colorado, the attackers hit the Department of Transportation demanding a $2m ransom payment.

This trend is particularly troublesome for government agencies and state run institutions in the UK and worldwide who are vulnerable by the mere fact that they could not afford to have the best and most up-to-date security systems and software because of financial cuts in the public sector.

The impact of the attack on Travelex can only be described as profound, bearing in mind the scale of the company's operations worldwide and the fact that, according to media reports, its employees were reduced to using the old fashioned pen and paper.

When businesses such as Travelex become victims of ransomware, it is vitally important to know how to react effectively.

From a legal and technical viewpoint, all businesses should arm themselves with pre-emptive legal protection and measures—the emphasis is very much on protection and preparation.

It is advisable for all businesses, irrespective of their size, to have a response plan ready to run, and particularly a ransomware recovery plan, which should be tested annually. Part of this plan—and this concerns companies who deal with large amounts of individual and corporate data such as Travelex—should be a back-up in the form of an offline central server that should be in place to store securely the most sensitive data. The existence of a secure server enables the victim company to recover its most precious commodity, data, thus blunting the need to pay ransom, and minimising the company's potential liability to class-action legal suits brought by individuals affected by that loss.

High stakes

For any company that has been the victim of a ransomware attack, the question to pay or not to pay the ransom becomes an existential one. Faced with such a predicament, it is important companies seek expert legal advice in how best to negotiate and navigate such troubled waters, as the stakes are high, and a right balance must be struck between protecting the company's reputation, recovering and securing the data, and getting the company back up and running again.

Presently, companies like Travelex, agonising about whether they should proceed to engage with the attackers, do so in a legal vacuum. It is noteworthy that there is no guidance given to companies from either the National Cyber Security Centre (NCSC—the technical authority on cyber security in UK) or the Financial Conduct Authority, (the regulator), on the issue of how to proceed. How are companies meant to conduct themselves negotiating with a highly sophisticated criminal enterprise? After all, extortion and blackmail are serious criminal offences that are non-negotiable and are normally resolved before a judge and a jury. And how are companies meant to make the payment if it is requested in bitcoin, for example? What is the legal status of such a payment? And doesn't the payment provide further fuel to the ransomware market itself?

Comment

Companies should become well versed in the type of threats that are out there, in terms of the ransomware being used and its capabilities. Learning from previous attacks is a useful step towards protection and prevention. An international 'bank' of threat intelligence, a catalogue/directory of ransomware variants, if you like, should be recorded and gathered from previous attacks and it should become part of the guidance available to companies.

It is time the UK government, through its agencies, took a clear stance nationally and internationally against this type of attacks, thus protecting the interests and rights of companies and creating a safer business environment. The FCA, in conjunction with the NCSC, the National Crime Agency, and expert cyber lawyers should fill this legal vacuum by creating specially tailored guidance to businesses faced with a ransomware attack and forced to make a payment. A 'rules of engagement' manual should exist to give clear guidance, and legal certainty to those affected. NLJ

Flavia Kenyon, barrister, 36 Commercial (*https://36group.co.uk/commercial*).