KCS Group Europe

Hacked off: the rise of ransoms for ransomware

25th July 2019

Norwegian conglomerate Norsk Hydro has spent £45 million GBP attempting to return to *'business as normal'* following a devastating cyber-attack that has taken out over 20,000 devices in 170 countries worldwide. Far from being an isolated incident, this extreme application of bad-actor cyber techniques to cripple some of the biggest companies in the planet is becoming more frequent – and the coping strategies are arguably exacerbating the problem, rather than solving it.

As much as £45m GBP may seem, Norsk Hydro has probably done the right thing in refusing to pay the ransom, even if it means a short-term loss of profits and a shift to manual operations (i.e., pen and paper). Paying criminals responsible for a ransomware attack is a poor idea for two reasons: firstly there is no guarantee that a targeted firm will ever get its data back (indeed once the principle of paying has been established, why not push that as far as possible?) – and secondly, it legitimises the very act of ransomware itself and the response to it. If ransomware is perceived by bad actors as somewhat profitable, they will explore it further and, rather than receding, the threat intensifies.

While the first point may be out of the hands of corporates and governments, the second is very much an active consideration and we appear to be heading in the wrong direction to combat it. Some firms are now actively paying the ransoms demanded, either openly or through the use of third parties (often cyber-security firms). Governments may not be willing to get involved, with the official lines generally being that paying ransoms is 'not encouraged', but these companies have no such obligations. To make matters worse, such payments are frequently made in cryptocurrency, rendering it even harder to track who the payments are going to – or their purpose (as cryptocurrency is commonly used in organised crime and funding of terrorism). But if paying ransomwares is seen as the easiest solution, this will serve only to increase the severity and frequency of strikes.

Or to give another recent example, the Florida Beach City Council has agreed to pay $600,000 USD after a three-week ransomware shutdown, and has approved a one-million-dollar investment to upgrade IT security *after* the fact. Their ransomware was delivered through a compromised link in a scam email. This doubles down on the situation – not only the submission to the bad actors in the first place, but the fact that ransomware does not require supreme tech skills to deliver. It is at the end of the day, a relatively low-complexity mechanism which has vastly inflated consequences (either in terms of the paralysis to a business or the pecuniary return).

Paying a ransom is not illegal, but at a time when ransomware is acknowledged by both governments and leading bodies in the UK and USA as the fastest growing and most serious cyber threat that SME companies are facing, the optics of paying up are not good. At best it encourages further crime, at worst it may actively facilitate organised criminal gangs and terrorism. The alternative then is to ensure that business continuity and backup plans are in place for any potential ransomware attack, so that if the worst happens the business will still be able to get back on track (albeit not costing upwards of £45m to do so – but that brings us on to a whole different discussion about cyber insurance!).

However, while prevention still remains far better than the need for a cure, the other alternative would be to remove the carrot and stick from ransomware situations. This would be, to allow affected corporates the ability to use third-party companies – the very ones that at present just facilitate the ransom – the ability to *'hack back'* and retrieve the lost data. At a stroke, all rationale for paying the ransom would be eliminated and the affected company could get back on track that much faster. Such a move seems unlikely to happen, but would represent a real change in the attitude of the British government to dealing with cyber threats. At present, everyone is paying – in more ways than one.