The growing threat of ransomware

https://www.icaew.com/insights/viewpoints-on-the-news/2021/aug-2021/the-growing-threat-of-ransomware?utm_campaign=Members%20-%20ICAEW&utm_medium=email&utm_source=1889486_ICAEWDaily_News_10August2021&utm_content=3&dm_i=47WY,14HXQ,KDBGB,54YBF,1

Author: ICAEW Insights

Published: 09 Aug 2021

Ransomware has been in the news a lot recently, but what is it? How can you avoid being a victim? And should you pay the ransom if you are attacked? The Tech Faculty's Kirstin Gillon explores some of the issues.

The basics of ransomware

A ransomware attack happens when hackers infiltrate systems, encrypt data and demand a ransom in return for the decryption key and access to the data again. Alternatively, hackers may claim to have stolen confidential data and threaten to publish it unless a ransom is paid. Ransoms are paid in cryptocurrency, usually bitcoin, largely due to the anonymity of crypto. Ransomware typically gets into organisations through phishing emails, where staff click on an infected link and download the malware. Alternatively, attackers can exploit vulnerabilities in software or use stolen Remote Desktop Protocol credentials to access networks and infect computers.

Ransomware attacks have grown hugely in recent years and the pandemic has increased the vulnerabilities of many organisations, with staff working at home and often using personal devices. This led the CEO of the UK National Cyber Security Centre, Lindy Cameron, to warn in June, "the primary key threat is not state actors but cyber criminals, and in particular the threat of ransomware." She went on to describe the professionalisation of the sector, with the rise of 'Ransomware as a service', making it very easy to commit attacks.

This has been reflected in a spate of high-profile incidents in the last 6 months. Colonial Pipeline made headlines when they were the victim of an attack in May, which led to fuel shortages in the US East coast for a few days. JBS Foods, the world's largest meat producer, was another victim, as was the Irish health service. Small businesses are also frequently targeted, as they often have poor security so can be easily attacked.

Should I pay?

So what do you do if you become the victim of such an attack and get a ransom request to get access to your data again, or stop the hackers publishing confidential information?

The official advice from the police and government is not to pay. They argue that there is no guarantee you will get your data back or that hackers won't publish data anyway. You will likely be funding other illegal activity. Furthermore, you would be encouraging further attacks, both on your own organisation and on others. As long as it is profitable for the attackers, the problem will only continue to escalate.

However, victims will usually be more focused on resolving their immediate crisis. Paying ransoms is not illegal and may well be cheaper than the cost of systems being down for a long period or having to rebuild systems. As a result, many companies do pay up, although there are no figures for how many do so. For example, Colonial Pipeline paid $4.4m in bitcoin to their attackers, some of which was subsequently recovered by the FBI.

Insurance can complicate the situation as insurers are reported to cover the costs of ransoms sometimes. The CEO of Colonial Pipeline testified to the US Congress that he discussed the ransom amount with their insurer and believed the insurer would cover the cost. Indeed, it is reported that

DarkSide, the group responsible for the Colonial Pipeline attack, researches potential victims' cyber insurance policies when deciding on the ransom amount.

Outlawing payments

So, should governments take the step of outlawing ransom payments, especially when payments are fuelling the rapid growth in ransomware attacks? Governments and law enforcement agencies seem reluctant to do so at the moment. They would rather that companies share information about ransomware with them, and making payments illegal would make that harder. Some companies would probably still pay and just factor in potentially paying an additional fine. So it may make little difference in practice and disproportionately hit smaller businesses.

Governments are also looking at bigger geopolitical solutions. Many of the current attacks come from countries such as Russia, and pressure can be applied at this level. It was reported, for example, the US President Biden broached the subject with Vladimir Putin at their recent summit.

The value of preparation and prevention

The best course of action for businesses, of course, is to avoid falling victim to an attack in the first place. Most attacks come via relatively unsophisticated methods, such as phishing emails, compromised credentials and unpatched systems. So getting in place good cyber hygiene and training staff properly are essential starting points for reducing the risks.

Having a good back-up strategy which is regularly tested is another key step. If you have a recent copy of systems and data that can be quickly reinstalled, you can take the sting out of the attack. Attackers will have thought of backups, though, and often target backups as well, so make sure backups are completely separate.

Then, have a recovery plan in place that has also been tested. While there are many examples of companies paying up, there are also examples of companies who refuse and are able to deal with the consequences. Sometimes the hackers are bluffing and don't go ahead and publish the information as threatened. And while recovery may take a while, it may be less costly than paying. The Scottish Environmental Protection Agency suffered a ransomware attack on Christmas Eve 2020, when 4,000 files were stolen, and were very public in their refusal to pay. 6 months on, they had restored the majority of their systems and fast-tracked a planned systems replacement as part of their recovery. They were clear that not paying was the right thing to do.

Resources

The NCSC has a wide range of resources to help organisations of all sizes to help improve cyber security. These include specific guidance on mitigating malware and ransomware attacks, questions for board members on ransomware, guidance on home working and the small business guide to cyber security.