S E C U R I T Y . . . .

Ransomware and the PIMBs sector

Ask anybody in charge of IT security the question "what is your biggest concern?" and either at the top of their list, or very close to it, will be ransomware. It has been around for many years and gained prominence in 2017 with the WannaCry outbreak – a global attack that exploited a vulnerability in Microsoft Windows. It resulted in significant impact to countless organisations and according to NHS England, affected 80 of its 236 trusts (either due to ransomware infection or IT teams proactively switching off devices).

Almost all organisations are at risk from ransomware. In Sophos' 'State of Ransomware in 2022' report, out of 5,600 mid-sized organisations across 31 countries that were interviewed, 66% had been the victim of ransomware in 2021. Professional institutes and memberships bodies will often hold thousands of sensitive records relating to members, so there is much to lose if attackers gain access to or renders them unusable.

Ransomware usually finds its way into networks via social engineering techniques, which dupe staff into opening infected email attachments or links...there will be very few organisations not regularly receiving suspicious emails! However, attackers will also try other means, such as guessing/cracking passwords and logging in via remote access systems or exploiting vulnerabilities in externally facing servers.

Whilst there is yet to be a follow-up on the same scale as WannaCry, ransomware and the attackers behind it are constantly evolving. When ransomware first became an issue, it generally required expert knowledge and sophisticated techniques to launch an attack. Shortly after the WannaCry outbreak, the UK's cyber security advisory body, National Cyber Security Centre (NCSC), attributed it as the work of 'state actors'.

Ransomware as a Service (RaaS) is a relatively new concept, in which developers of ransomware tools hire them out to less sophisticated attackers, with both parties taking a share of any ransom payments. Some of these organisations have a surprising amount of structure to them, with HR, recruitment, comms teams, and the provision of technical support services to those hiring their tools.

However, the most worrying change to ransomware has been the use of double extortion techniques. Previously, if an organisation became a victim of an attack, as long as there was an effective backup strategy in place, the ransom note could be ignored, data restored, and operations continued. However, many attacks now incorporate an initial phase of copying victim's data to an external location prior to it being encrypted (referred to as 'data exfiltration'). The ransom note will then demand payment not only to recover data, but also to ensure it is not released to the public. Organisations will be alarmed at the thought of sensitive member data being leaked on the Internet, with the reputational, financial, and regulatory risks being significant.

Whilst being attacked might seem like an inevitability to some, there are ways of minimising the risk. Generally, when attacks are successful, it involves multiple process, human or technical control failures – it is rare for only one thing to have gone wrong.

At the top of the list should be ensuring that IT teams have put appropriate controls in place, they are working effectively and, as important, are tested on a regular basis. NCSC provides excellent guidance for senior management and board members, explaining what ransomware is and the types of questions to be raising with their IT teams.

They also provide practical resources, help and cyber security training content for small and medium sized organisations, available here.

Another area for consideration is implementing a security framework, such as the government backed Cyber Essentials (CE) and Cyber Essentials Plus certification – a prescriptive set of controls designed to protect organisations from the most common form of cyber-attacks. CE is also a great way of demonstrating to members that cyber security is taken seriously – you can find out more here.

Cyber insurance policies with ransomware cover can be useful in the event of an attack, and historically insurers have generally paid out when required. However, with the ongoing rise in the number of attacks, premiums are increasing, restrictions on cover are being applied and insurers are demanding that organisations have effective security controls in place.

Cyber security improvement should be an embedded process within all organisations and risk assessments should be kept updated to deal with ransomware and other cyber threats. A plan should then be created to prioritise the implementation and improvement of controls and to coordinate associated spend.

Simon Bulleyment
Director, Sibrossa Ltd
07899 842488
sbulleyment@sibrossa.com