Picture credit: AdobeStock

MILITARY MINDSET

Tom Exelby *reveals why SMBs need to change their thinking to combat the menace of ransomware*

Small and medium-sized businesses (SMBs) in the UK are high-profile targets for cyber criminals – and the constant evolution of ransomware is one of the severest challenges. A survey of 2,000 SMBs in the UK and US by Microsoft in September last year, for example, found cyber criminals have attacked one in three firms. The average cost of investigation and recovery after an attack was anything between £60,000 ($78,000) and £3.1-million ($4-million), with an average of £191,000 ($250,000).

Although ransomware is just one type of malware, it is the intended threat of extortion, system down time and data theft that packs the biggest punch, capable of inflicting fatal damage. To defend themselves, SMBs need a reinvigorated approach, going back to the cyber basics and extending their effectiveness through methodologies borrowed from the military.

While SMBs have been paying close attention to data protection and strengthening their ability to detect phishing attacks, they should ensure they have no blind spots in relation to ransomware because the consequences of failure are so severe.

The costs of ransom payments to have data decrypted followed by remediation and recovery are mounting all the time. The loss of reputation among customers, partners and suppliers is a significant cost on its own. Irrespective of whether SMBs pay ransoms to have data restored, prolonged downtime caused by an attack can be enough to destroy a business. The haulier KNP Logistics, for example, was put out of business by Russian ransomware attackers in 2023 with the loss of hundreds of jobs because its data remained encrypted.

The danger for SMBs is underestimating the deviousness of ransomware criminals. While almost all the SMBs surveyed by Microsoft agreed cyber security is critical, 72 percent saw data protection as a challenge compared with only 42 percent identifying ransomware.

SMBs need to revitalise their approaches to ransomware because they lack in-house time and expertise, which puts them at a substantial disadvantage when up against ransomware gangs employing many new techniques including generative AI to increase speed and accuracy.

IBM's 2024 X-Force Threat Intelligence Report highlights how credential and identity-based threats are growing. Phishing, using stolen and valid credentials is more sophisticated while social engineering, password-breaking software or keystroke logging are all methods that gangs continue to employ. Many of these tactics are precursors to ransomware attacks.

SMBs should ensure they have no blind spots in relation to ransomware because the consequences of failure are so severe.

This year's CrowdStrike Global Threat Report confirms that 2024 saw the evolution of threats employing "high-tempo social engineering, legitimate remote tools and cloud-hosted payloads" to bypass defences. CrowdStrike found these techniques, including phoney help desk calls, are in use by groups including the outfit behind Black Basta ransomware. The report highlights how the time it takes attackers to move through a target's network once they have gained entry has crashed from 48 minutes to 51 seconds – a huge drop.

These developments accompany changes in the ransomware underworld, where the barriers to entry have been lowered through ransomware-as-a-service and a system of sub-contracting and specialisation. Ransomware is extremely attractive because it has low investment compared with other forms of organised crime and carries far less risk of being caught. The FBI estimates the Akira gang that targeted KNP Logistics raked in $42-million from just 250 attacks.

SMBs may feel they are too small to be of interest to ransomware gangs. But this is where the criminals are clever. They use a formula to calibrate their demands according to the size of the business' revenue and they have malware that can access a company's insurance policy to work out the maximum level of extortion likely to trigger a pay-off.

To deal with such cunning adversaries, SMBs need to adapt their cyber security posture so they can constantly adapt to the new or updated techniques that criminals deploy. Rolling out a single solution and then relying on it to provide all-round protection is not effective in today's adversarial environments. Ransomware gangs are always tunnelling under or finding new paths through static, perimeter defences.

The experience of UK cyber security companies shows many SMBs still practise poor cyber hygiene, failing to do the basics such as regularly changing passwords, implementing multi-factor authentication and consistently applying security patches to software to remove vulnerabilities. Even security awareness training is frequently neglected, which is extremely dangerous given that the human factor is so prevalent in cyber breaches. Last year's Verizon Data Breach Investigation Report, for example, found a human element in 68 percent of breaches. The success of phishing campaigns is often a result of staff being unaware of what to spot in an email that indicates it contains malicious content. Firms that are still struggling with the essentials in this way should make a concerted effort to comply with the NCSC's Cyber Essentials programme, which is a major step in the right direction without significant cost.

An important element in the basics of cyber defence is resilience. Organisations must gain a greater understanding of resilience and use external expertise so they can not only defend, but also respond and recover from an attack as quickly as possible. Achieving effective resilience requires military precision, with a detailed and rehearsed incident response plan which addresses the key tenants of containment, eradication and recovery.

Planning for a ransomware attack must include mapping of data and a thorough understanding of its sensitivity. In other words, whose data it is and who may have to be informed – such as customers and third parties. This is important for regulatory compliance, but also to avoid long delays and indecision in the event of a ransomware attack. Any failure to inform affected individuals or companies is likely to incur reprimands and possibly, penalties from the Information Commissioner's Office or regulators.

For business continuity, organisations must regularly review their backup policies. Securing backups is essential as ransomware attacks frequently commence with encryption of backups before the criminals move on to their main targets.

ONE IMPORTANT LESSON FROM THE MILITARY SPHERE IS REGULAR DRILLS AND EXERCISES

The three watchwords here are defend, respond and recover, requiring a multi-layered ecosystem of tools that will kick in at different stages of an attack. This is where SMBs should learn from the military sector and adopt a layered defence in-depth approach.

Unfortunately, many SMBs put almost total faith in their endpoint protection. Even when they have integrated solutions behind them, nobody is monitoring, which significantly reduces their efficacy. Monitoring of endpoints is a necessity, but it must be in line with risk-management protocols that fit the business and its requirements. This requires expertise to know which alerts matter and how to act on them.

Fortunately, there is an optimal approach which utilises behavioural analysis to identify the telltale signs of a ransomware intrusion and stop it in its tracks. Spotting this behaviour is possible due to the nature of a ransomware attack and the predictable pathway it needs to take through a digital system to achieve its aim. If ransomware has been undetected and successfully starts to encrypt data, more advanced tools will recognise this, stop the process and be able to decrypt the small amount of encrypted data. This removes the necessity for negotiations, payments and prolonged downtime while backups are restored.

Given the speed with which ransomware can move through systems, SMBs must also segment their networks through user permissions. This will slow down lateral movement and increase the likelihood of detection. Multi-factor authentication is not difficult to implement and creates a significant barrier for attackers attempting to use compromised credentials. It is a simple but effective step.

SMBs need to act now because although the threat from AI is easily overstated, it is improving the effectiveness of ransomware, especially in the initial techniques that precede an attack. All the evidence shows AI is gradually making phishing campaigns faster and better targeted. With large language models, criminals can scan through masses of data

– including stolen data – for the target details most relevant to their phishing campaign. Then they can prompt the technology to use these details to devise better-worded, more convincing emails that act as lures.

THE DANGER FOR SMBS IS UNDERESTIMATING THE DEVIOUSNESS OF RANSOMWARE CRIMINALS

This is not where the use of AI ends, however. AI will help criminals identify organisations that have been lax about patching a particular vulnerability and can point to the open doors in a network. If a vulnerability is patched, adapting the malware to find another vulnerability is relatively straightforward for practised operators. This is why regular patching is now so important.

Criminals are deploying AI to accelerate scanning for weaknesses once they are in an organisation's environments. They scan data to work out what is most important to a firm, examine the insurance certificate to gauge its size and coverage, and determine the likelihood and size of a payout. The speed of these operations, followed by encryption, makes it harder for businesses to detect without specialist tools and external expertise.

There are lessons here for businesses from the military approach to risk-management, tying together people, processes and technology. SMBs need intelligence about what their enemies are doing – in this case it is the ransomware gangs. This intelligence should include information about how other organisations have been breached and what happened – what was successful and what was not. The business must use this intelligence to inform their defence, making an attack as difficult as possible by, for example, patching vulnerabilities as soon as possible. It is important not just to monitor for new threats, but to act on them, following the military concept of intelligence integration.

Allied to this is resource prioritisation – the process of focusing potentially limited resources on the most important, most lethal threats. This demands experience to avoid creating new threats through undue focus on one area. Concentrating on ransomware should not rob an organisation of effective defences against other types of threats.

Another important lesson from the military sphere is the necessity for regular drills and exercises. The ability to react decisively and recover quickly from a ransomware attack depends in large measure on preparation and the development of well-rehearsed, documented processes that people know how to follow should a breach occur. Making these drills effective demands thorough analysis of their effectiveness, followed by fast adaptation to ensure continuous improvement.

The dangers of ransomware are unlikely to recede for the UK's SMBs, given the profitability of this area of cyber crime, the increased sophistication and specialisation of the gangs involved and the low likelihood of them being caught. Yet, as we have seen, there are steps that SMBs can take that involve basic cyber hygiene and adoption of a multi-layered defence. With the assistance of third-party expertise, there are many reasons why SMBs should feel able to protect themselves against the menace of ransomware ●

Tom Exelby is Head of Cyber Security at Red Helix.

The time it takes attackers to move through a target's network once they have gained entry has crashed from 48 minutes to just 51 seconds

Picture credit: AdobeStock