The Economist

Five best practices for securing data from ransomware

As ransomware becomes increasingly sophisticated, here are some steps that businesses can take to prevent damage.

Ransomware is big business. Malware encrypts files and computers, making them impossible to access unless a payment is made, and can cripple companies. "I see ransomware continuing to evolve in complexity and sophistication," says Danny Allan, vice-president of product strategy at Veeam, a global data management firm.

Ransomware should be taken seriously as it can have huge implications for companies. Not only can data be lost, but regulatory action following a cyber-attack can result in fines. It can also result in reputational damage with customers, who may lose trust in the company.

"The scale and automated nature of a ransomware attack makes it profitable through economies of scale, rather than through extorting large amounts from targeted victims," according to the UK's National Cyber Security Centre (NCSC), which is responsible for helping businesses to stay safe. "They are attacks of opportunity."

Steps can be taken, however, to limit the damage that ransomware could have if a business is targeted. Mr Allan, a former cybersecurity professional who now specialises in data management solutions and data protection for Veeam, highlights five best practices that companies should follow.

1. KEEP A CLEAN COPY OF THE DATA

Mr Allan says that businesses should keep at least three copies of their data: a version that is being worked on and two back-ups. When it comes to ransomware, keeping one of these back-ups offline is key. "Every organisation must realise that the last line of defence is to have a clean copy of the data that is not network-connected," he adds.

By keeping one copy of a company's data offline, it vastly increases the likelihood that ransomware will not be able to reach it, allowing systems to be restored from this copy. If a company is hit by a ransomware attack, Mr Allan adds, the uninfected offline copy of the data should be replicated as quickly as possible.

2. STOP DEVICES RECEIVING MALWARE

Actions can be taken to stop ransomware infecting networks in the first place. The NCSC says there are a number of ways to "reduce the likelihood of malicious content reaching your network". These include whitelisting file types, blacklisting suspicious websites, and using signatures to block known malicious code. It also adds that email filtering, safe browsing limits and actively using software to inspect content can help limit the potential of ransomware.

3. REDUCE PRIVILEGES

"Too many organisations allow administrative access, meaning that anyone has full access to everything: whether it be databases or applications," says Mr Allan. He recommends that businesses regularly review who has access to what files and which systems to determine whether the correct permissions are in place.

4. EDUCATE EMPLOYEES

Ransomware often finds its way into corporate systems because of an individual clicking on, or running, a piece of dangerous code. "We regularly find that end users are the weakest link," Mr Allan says. Both he and the NCSC say that people should be trained to understand best practices, such as spotting potential malware and suspect behaviour.

Even education on simple cybersecurity measures can help companies. "Employees—because they like mobility and are connected to their corporate systems all the time—sometimes do not realise that they should behave differently on a corporate network than on a public Wi-Fi network," Mr Allan adds.

5. RUN TESTS ON YOUR DATA

"One of the key things that you can do proactively is to take copies of your data systems and to test them for vulnerabilities," Mr Allan says. It is possible to create sandboxes—walled off areas where experimentation can happen—to simulate ransomware attacks and find weaknesses in systems. These can be used to analyse how susceptible a data system is to already-known attacks.

According to Mr Allan, criminals developing ransomware will continue to push the boundaries of what they can do technically. Ransomware will only become more sophisticated in the coming years and, he says, it is essential for companies to use best practices to help protect the data they hold.