BE AWARE OF RANSOMWARE

CYBER SECURITY
COOPERATIVE
RESEARCH
CENTRE

As the Covid-19 pandemic has swept across the world, another less visible epidemic has occurred concurrently—a tsunami of cybercrime producing global losses totalling more than US$1 trillion. While cybercrime is huge in scale and diverse in form, there's one type that presents a unique threat to businesses and governments the world over: **ransomware.**

WHAT IS RANSOMWARE?

Ransomware is a form of malware designed and deployed by cybercriminals who seek out vulnerabilities in the computer systems of organisations, both large and small, locking up, encrypting and extracting data. This renders computers and their files unusable. Attacks are accompanied by a demand for ransom to be paid in return for decrypting and unlocking systems.

Increasingly, ransomware attacks include an extortion element that involves threats to leak stolen data publicly or on the dark web if payment isn't made (known as 'hack and leak'). This exerts extra pressure on the victim to pay the ransom. The most common way ransomware is deployed into a system is via email phishing campaigns, remote access vulnerabilities and software vulnerabilities.

Ransomware attacks are entirely foreseeable and almost always defendable. In the physical world, organisations pay for security alarms, high fences and sensors to protect their property. The digital world should be no different.

DO AUSTRALIANS UNDERSTAND WHAT RANSOMWARE IS?

25% said ransomware was the most significant cybersecurity threat to Australian businesses, coming in behind hacking (48%)

75% said they wouldn't know what to do if they fell victim to a ransomware attack

56% said they would contact the ACSC when given a set of options if they fell victim to a ransomware attack

42% said they understood how a ransomware attack occurred

44% indicated that they knew what happened in a ransomware attack

71% respondents believed financial gain was the key aim of an attack (71%), followed by data theft (14%)

THREE BASIC STEPS TO PROTECT YOUR ORGANISATION AGAINST RANSOMWARE

1. Patch, patch, patch

Patch management is essential for effective cybersecurity and ensures the security features of software on computers and devices are up to date. All software is prone to technical vulnerabilities and, when a vulnerability is exposed and shared, cybercriminals have a metaphorical front-door key.

2. Multi-factor authentication (MFA)

MFA is a security measure that requires two or more proofs of identity to grant access to a system. It offers significantly more powerful security and protection against cyber criminals because even if they manage to steal one proof of identity still need to obtain and use the other proofs of identity to access an account.

3. Employee cyber education

Cybercriminal only need to trick one person to gain access to a system. Lures, like phishing emails containing malicious links, are commonly used to deploy ransomware. Therefore, training employees to be better prepared to identify suspicious emails— and not to click on them— is essential.

For more information about ransomware or if you are the victim of a ransomware attack contact the Australian Cyber Security Centre on 1300 CYBER1 (1300 292 371) or visit www.cyber.gov.au/ransomware.