RANSOMWARE RESILIENCE TIPSHEET

In 2020, over two-thirds of Australian businesses suffered a ransomware attack, with a third of these victims paying the ransom*. But what can businesses be doing to protect themselves against these attacks?

URL CLICK-TIME PROTECTION

Controls within your Secure Email Gateway to evaluate links in real-time both before email delivery and again at the time of click, blocks malicious links.

SANDBOXING CONTROLS

Provides an isolated environment to execute files and URLs before they are opened on the production network.

SECURITY AWARENESS TRAINING

Teach your employees how to spot a potentially malicious email and what to do with them.

WEB THREAT ISOLATION

Block file uploads and downloads to uncategorised and security-risk websites as well as block forms association with phishing sites.

SHARED THREAT INTELLIGENCE

Utilising native integrations to share indicators of compromise and other threat intelligence across your security solutions.

ENDPOINT DETECTION & RESPONSE

Artificial intelligence and machine learning is leveraged to record, investigate and analyse endpoint activity. Delivering real-time protection by automatically identifying and remediating threats.

+612 9221 5555 info@infotrust.com.au www.InfoTrust.com.au

InfoTrust

WHAT CAN YOU DO
IF YOU DO FALL VICTIM TO RANSOMWARE?

DISCONNECT THE INFECTED DEVICE

Disable WiFi, network and data cables, USBs and Bluetooth

GATHER KEY INFORMATION

Pull together screenshots, details on how the malware was deployed and the attack chain

REACH OUT TO AN EXPERT

Once you've gathered all the pertinent information contact an expert who will be able to assist you in removing the ransomware

RESTORE YOUR DATA FROM BACK UPS

More than likely once the malware is removed you will need to restore your company data. This is why robust back ups are a key strategy to remaining cyber resilient against ransomware attacks

*CrowdStrike 2020 Global Security Attitude Survey

+612 9221 5555 info@infotrust.com.au www.InfoTrust.com.au

InfoTrust