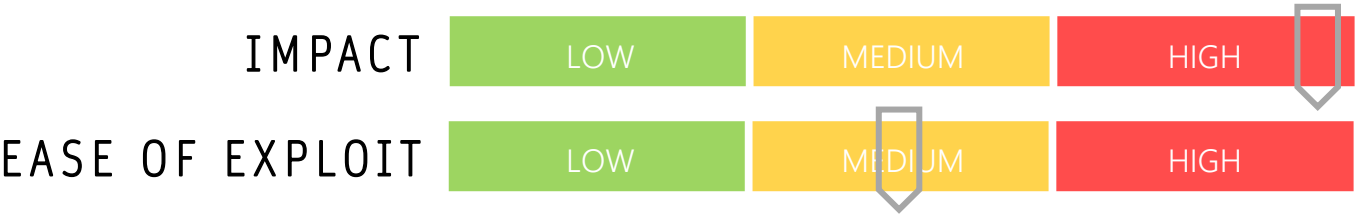
UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 0005

RANSOMWARE – KEY THREAT FOR 2020

DATE ISSUED: 28th June 2020



OVERVIEW

Predictions for a surge in Ransomware to hit New Zealand Businesses and US and European targets make it more difficult for attackers to be successful through investment in technology, insurance and awareness training.

BREAKDOWN

Common methods of infiltration include exploitation of vulnerabilities on perimeter devices and delivery of malware through email or Internet Query Files. More sophisticated attacks, high ransom fees and threats to publish or sell exfiltrated information make new ransomware attacks an ever increasing threat and paying the ransom will not guarantee locked files can be decrypted or data fully recovered.

REMEDIATION STEPS

- Ensure your organization has up to date Business Continuity and Disaster Recovery Plans
- Check your backup reports and routinely test restore procedures
- Create archive backups and ensure they are updated at regular intervals using varied backup types and have at least one copy stored offsite and offline
- Provide information and training to all employees regarding social engineering and phishing, how to spot an attack and what to do if an attack is suspected.
- Check network device security, access control permissions and open ports and monitor for abnormal activity
- Implement security-in-depth/defense-in-depth multilayered protections
- Check home network security and password policy compliance for those working from home.

REFERENCES & RESOURCES

Stuff: https://www.stuff.co.nz/business/121915739/tsunami-of-ransomware-attacks-coming-businesses-warned
Reseller News https://www.reseller.co.nz/article/671235/ransomware-costing-new-zealand-up-41m/
Security Brief https://securitybrief.co.nz/story/ransomware-attacks-swell-average-ransom-payments-rise-report
Trend Micro https://www.trendmicro.com/vinfo/nz/security/news/cybercrime-and-digital-threats/investigation-into-a-nefilim-attack-shows-signs-of-lateral-movement-possible-data-exfiltration