beazley

RANSOMWARE SUPPLEMENTAL APPLICATION

E-MAIL SECURITY

1. Do you pre-screen e-mails for potentially malicious attachments and links? ☑ Yes ☐ No

2. Do you provide a quarantine service to your users? ☐ Yes ☐ No

3. Do you have the capability to automatically detonate and evaluate attachments in a sandbox to determine if malicious prior to delivery to the end-user? ☐ Yes ☐ No

4. Do you strictly enforce Sender Policy Framework (SPF) on incoming e-mails? ☐ Yes ☐ No

5. How often is phishing training conducted to all staff (e.g. monthly, quarterly, annually)? ____________

6. Can your users access e-mail through a web app on a non-corporate device? ☐ Yes ☐ No

   If Yes: do you enforce Multi-Factor Authentication (MFA)? ☐ Yes ☐ No

7. Do you use Office 365 in your organisation? ☐ Yes ☐ No

   If Yes: Do you use the o365 Advanced Threat Protection add-on? ☐ Yes ☐ No

INTERNAL SECURITY

8. Do you use an endpoint protection (EPP) product across your enterprise? ____________

9. Do you use an endpoint detection and response (EDR) product across your enterprise? ____________

10. Do you use MFA to protect privileged user accounts? ☐ Yes ☐ No

11. Is a hardened baseline configuration materially rolled out across servers, laptops, desktops and managed mobile devices? ____________

12. What % of the enterprise is covered by your scheduled vulnerability scans? ______

13. In what time frame do you install critical and high severity patches across your enterprise? ____________

14. If you have any end of life or end of support software, is it segregated from the rest of the network? ____________

15. Have you configured host-based and network firewalls to disallow inbound connections by default? ____________

16. Do you use a protective DNS service (e.g. Quad9, OpenDNS or the public sector PDNS)? ☐ Yes ☐ No

17. Do you use an endpoint application isolation and containment technology? ____________

18. Do your users have local admin rights on their laptop / desktop? ☐ Yes ☐ No

19. Can users run MS Office Macro enabled documents on their system by default? ____________

20. Do you provide your users with a password manager software? □ Yes □ No

21. Do you manage privileged accounts using tooling? E.g. CyberArk ______________

22. Do you have a security operations center established, either in-house or outsourced? ______________

BACK-UP AND RECOVERY POLICIES

23. Are your backups encrypted? ______________

24. Are your backups kept separate from your network ('offline'), or in a cloud service designed for this purpose? ______________

25. Do you use a Cloud syncing service (e.g. Dropbox, OneDrive, SharePoint, Google Drive) for backups? □ Yes □ No

26. Have you tested the successful restoration and recovery of key server configurations and data from backups in the last 6 months? ______________

27. Are you able to test the integrity of back-ups prior to restoration to be confident it is free from malware? ______________

OTHER RANSOMWARE PREVENTATIVE MEASURES

Please describe any additional steps your organization takes to detect and prevent ransomware attacks (e.g. segmentation of your network, additional software tools, external security services, etc.).

Digital signature required below [click the red tab to create a digital ID or import an existing digital ID]:

Signed: ______________________________________

Print Name: ______________________________________

Title: ______________________________________

Company: ______________________________________

Date: ______________________________________