Ransomware
Prevention and Response Checklist

Ransomware **prevention checklist**

Preventive measures at the user level

- [ ] Conduct security awareness training and educate your end users about ransomware attacks.
- [ ] Train your end users to spot and report phishing emails containing malicious attachments.

Preventive measures at the software level

- [ ] Ensure your firewalls are operational and up-to-date at all times.
- [ ] Logically separate your networks.
- [ ] Employ a strong email filtering system to block spam and phishing emails.
- [ ] Patch vulnerabilities and keep all your software updated.
- [ ] Set up rigorous software restriction policies to block unauthorized programs from running.
- [ ] Keep your antivirus fully operational and up-to-date.
- [ ] Conduct periodic security assessments to identify security vulnerabilities.
- [ ] Enforce the principle of least privilege.
- [ ] Disable Remote Desktop Protocol (RDP) when not in use.
- [ ] Disable macros in your Microsoft Office files.
- [ ] Use a strong, real-time intrusion detection system to spot potential ransomware attacks.

Preventive measures at the backup level

- [ ] Back up your files using a 3-2-1 backup rule, i.e. retain at least three separate copies of data on two different storage types, with at least one of those stored offline.
- [ ] Ensure that you back up critical work data periodically.
- [ ] Enforce regular checks for data integrity and recovery on all your backups.

Ransomware response checklist

Time-sensitive reactive measures

- [x] Shut down infected systems immediately.
- [x] Disconnect and isolate infected systems from the network.
- [x] Isolate your backups immediately.
- [x] Disable all shared drives that hold critical information.
- [x] Issue an organization-wide alert about the attack.
- [x] Contact your local law enforcement agency and report the attack.

Analysis-based reactive measures

- [x] Determine the scope and magnitude of an infection by identifying the type and number of devices infected, as well as what kind of data was encrypted.
- [x] Determine the type and version of the ransomware.
- [x] Identify the threat vector used to infiltrate your network.
- [x] Conduct root cause analysis.
- [x] Mitigate any identified vulnerabilities.
- [x] Check if a decryption tool is available online.

Business continuity reactive measures

- [x] Restore your files from a backup.

Contact your trusted technology partner Danush in case you need any support in setting up **Preventive System or Responsive System** for your data security.

Call Now

M N Smitha – Service Co-Ordinator | +91 9980139541 | support@dhanush.com