Malware prevention tips for businesses

www.thecyphere.com

info@thecyphere.com

MALWARE

=

MALicious + softWARE

Ransomware is a type of malware

Learn pragmatic ways to prevent malware and ransomware

1. Prevent malware delivery

Reduce the likelihood via secure remote access

- Enable secure MFA config
- Use VPNs
- Implement network segmentation
- Monitor for suspicious activity and anomalies

Email & web filters such as

- Blocking the malicious emails and removing executable attachments.
- Intercepting proxies
- Internet security gateways
- Safe browsing lists within browsers

User education

- Encourage detection and reporting of incidents.
- Promote use of password managers, passwordless mechanisms where possible.

2. Restrict malware infection

Secure OS configuration

- Configure necessary features and services.
- Limit user permissions.
- Block unauthorised network traffic via firewall.
- Review and harden OS settings.

Patch management

- Update OS and software promptly.
- Use automated patch management tools.
- Regularly scan for vulnerabilities and mitigate using risk focussed approach.

Restrict scripting and macros

- Apply constrained language mode.
- Allow macros only from trusted sources.
- Disable autorun for mounted media.
- Use an anti-malware product that integrates with AMSI.

3. Limit malware impact

Least privileges

- Only provide the necessary permissions aligned with functional requirements.
- Follow strict approval processes for privileges.
- Conduct regular reviews of user permissions.

Permission reviews

- Remove excessive or outdated permissions.
- Ensure RBAC.
- Audit permissions.
- Isolate legacy or unsupported systems.

Segregating obsolete systems

- Disconnect from the network.
- Implement firewalls.
- Plan for system upgrades or replacements

Conduct regular security reviews to validate your controls.

4. Education

Zero exceptions

- Instill a culture of zero tolerance for malware.
- Encourage personal cybersecurity responsibility.

Regular training

- Conduct security training.
- Promote safe online practices.
- Educate on malware prevention.

Considering your Supply Chain

- Extend security to partners.
- Vet vendor security.
- Enforce access controls.
- Continuously monitor supply chain security.

5. Backup

Utilising the cloud for backup

- Use cloud storage for scalability.
- Automate backups for sync.
- Encrypt data before upload.

Testing backups

- Test backup restoration regularly.
- Verify completeness and accuracy.
- Conduct partial and full recovery tests.

Keeping offline backups

- Use offline backups on physical media/separate zones (cloud only).
- Isolate them from the network.
- Regularly update and verify offline backups.

LIKE THIS?

☑ Follow and repost ♻️

☑ Should you need to discuss your security needs, get in touch:

www.thecyphere.com
info@thecyphere.com