PALINDROME CONSULTING®

Ransomware Runs Rampant In The Business World — Do You Know How To Defend Your Company?

Ransomware is a type of malware that encrypts the target's data *(making it unreadable and inaccessible)* and holds it for ransom. It targets all data on the target's systems, making it impossible for them to ignore until they pay the ransom, or wipe the data.

That's why any protective measures you employ should help to limit the possibility of ransomware entering your systems, as well as providing redundancies for when it does.

Your Ultimate Ransomware Defense Checklist

□ Confirm that anti-malware and antivirus settings are deployed to automate all updates and to continually conduct system and device scans.

□ Have a policy in place that verifies software updates are being applied in a timely manner. Unpatched software can be exploited by cybercriminals to infect your systems with malware.

□ Ensure you have 24/7 oversight of your network to identify and address potential security issues before they take effect.

□ Access controls should be configured so that shared permissions for directories, files and networks are restricted. The default settings should be "read-only" access to essential files, with limited permissions for write access to critical files and directories.

□ Implement Multi-Factor Authentication to protect accounts from access with breached passwords

□ Train your staff to ask themselves these key questions before opening an email:

- Do I know the sender of this email?
- Does it make sense that it was sent to me?
- Can I verify that the attached link or PDF is safe?
- Does the email threaten to close my accounts or cancel my cards if I don't provide information?
- Is this email really from someone I trust or does it just look like someone I trust?
  What can I do to verify?
- Does anything seem "off" about this email, its contents or sender?

□ Disable:

- Macro scripts in email
- Files running within AppData or LocalAppData folders
- Remote Desktop Protocol capabilities *(unless needed, in which case they should be limited to internal network use)*

□ Software restriction policies should be created or other controls implemented that prevent the execution, especially in the common locations where ransomware lurks, such as temporary folders used by the most common web browsers.

□ Have an annual security audit and penetration test performed to determine how vulnerable your organization is.

□ Data backup best practices:

- Back up data on a regular basis *(at least daily)*.
- Inspect your backups to verify that they maintain their integrity.
- Secure your backups and keep them independent from the networks and computers they are backing up.
- Maintain air-gapped backups to prevent spreading ransomware infections.

Need Expert Assistance With Your Ransomware Defense?

When you're not sure if you have the skills or knowledge to get the job done, what can you do? Consult with cybersecurity professionals like those on the **Palindrome Consulting** team.

Our job is to manage your cybersecurity, simple as that. Instead of needing an employee or internal team to keep your tech and data secure, you let our team do it for you.

Get in touch with our team to get started on your ransomware defense today.

PALINDROME
PCR
CONSULTING®

(305) 944-7300 | www.pciicp.com