Heavy Vehicle Cyber Security Updates

National Motor Freight Traffic Association, Inc.
1001 North Fairfax Street, Suite 600
Alexandria, VA 22314
(703) 838-1810

October 12, 2020

October is National Cybersecurity Awareness Month (NCSAM). This is a collaborative effort between the US Department of Homeland Security (DHS) Cybersecurity Infrastructure Security Agency (CISA) and its public and private partners. As contribution to this effort, NMFTA is providing you with our Top 10 tips on how to protect your company against ransomware. While nothing is absolutely certain, following these 10 steps should help you prepare and defend against ransomware.

Top 10 Tips to protect against ransomware

1. Backup data regularly and, more importantly, routinely confirm restoration from backups.
2. Maintain 'cold' (off-line) backup snapshots of complete system images with long rotations, i.e. weekly offline backups maintained for two months.
3. Have an Incident Response (IR) plan; keep printouts of this plan. When the worst happens, follow the plan. The plan should include printouts of build instructions for setting up and configuring your endpoints and critical server infrastructure from scratch in case you have to rebuild from the ground up.
4. Deploy edge security appliances such as firewalls with IDS/IPS and email security gateways and monitor their event logs and alerts. Most malware comes in via email, so a layered perimeter email defense goes a long way.
5. Patch all operating systems, applications, browsers, etc. at least every 30 days. Consider subscribing to the CISA weekly vulnerability list to keep up to date on latest developments [https://public.govdelivery.com/accounts/USDHSUSCERT/subscriber/new].
6. Run vulnerability scans and mitigate found issues at least every 30 days.
7. Do not expose Remote Desktop Protocol (RDP) directly on the internet.
8. All remote VPN access should require multi-factor authentication and endpoint rules (e.g. domain membership, etc.).
9. No regular user account should have admin privileges to any computer (use separate accounts with 2 factor for admin access). This also applies to system administrators. You don't need to be a domain admin to check your email.
10. Run up-to-date malware and anti-virus software as well as monitor activity and events logs on all endpoints and servers.

Bonus Materials: See useful resources at http://www.nmfta.org/pages/RansomwareResources