EINPRESSWIRE

Five Tech Tips from Hyperion Networks to Prepare East Tennessee Businesses for Ransomware Season

LOUISVILLE, TN, UNITED STATES, June 26, 2025 /EINPresswire.com/ -- At Hyperion Networks, the changing patterns in cyberattacks across East Tennessee have been observed with concern, particularly the rise in ransomware incidents during the summer and fall months. As IT service providers who work closely with small and mid-sized businesses in the region, attention is being drawn to the vulnerabilities that often go unnoticed until after a breach has occurred.

The increased targeting of local companies has been noted, especially those relying on aging infrastructure or under-maintained software. Hyperion Networks has seen firsthand how the fallout from ransomware attacks can disrupt operations for weeks and leave businesses scrambling to recover critical data. In many cases, these disruptions could have been reduced, or entirely avoided, through timely preventative action.

A major focus has been placed on backup strategies. Systems that are backed up inconsistently or stored on the same network as live data are being exploited more frequently. Off-site backups that are routinely tested for integrity have proven far more reliable in recovery scenarios. Alongside this, attention is being paid to employee access controls. It has been found that over-permissioned user accounts are commonly used as entry points for ransomware payloads, often through phishing emails.

Regular patching of software and operating systems remains one of the most overlooked steps in network defense. When patches are missed, vulnerabilities stay open, and attackers are quick to use them. At Hyperion Networks, patch management has been emphasized for every client system, no matter how minor the update may appear.

Multifactor authentication is now being seen not as an extra layer, but as a required baseline. Systems protected by a single password have been increasingly breached, with credential reuse across platforms being exploited more often. Businesses that have adopted multifactor authentication have faced significantly fewer intrusions.

Lastly, cybersecurity awareness among staff has been prioritized. Ransomware frequently gains its first foothold through user error, typically by clicking malicious links or downloading compromised files. Businesses whose employees have been trained to spot suspicious content have seen incident rates drop substantially.

At Hyperion Networks, it is believed that a proactive, methodical approach to cybersecurity serves East Tennessee businesses far better than reactive measures taken after damage has already been done. By keeping systems maintained, access limited, and users informed, the region's businesses can be better protected from what has become an increasingly aggressive and costly threat.

Micheala L. ray
Hyperion Networks
email us here
Visit us on social media:
LinkedIn
Facebook
X