CERTES BLOG

Responding to Ransomware with the DHS Cyber Hunt & Incident Response Teams Act

RESPONDING TO RANSOMWARE WITH THE DHS CYBER HUNT & INCIDENT RESPONSE TEAMS ACT

October 2019

A new law has passed the US senate this week which will demand the federal government to heighten its support for organizations hit by ransomware. Ransomware is currently on the rise, with cyber-attacks on businesses up by 365% in 2019 as cybercriminals move their focus to businesses rather than consumers, hoping for a "big payout".

The Department of Homeland Security (DHS) Cyber Hunt and Incident Response Teams Act would require the DHS to give advice on how best to protect systems from cyber-attacks. If the bill is passed, the DHS would be expected to build dedicated teams to provide this advice, as well as other technical support, including incident response assistance. In addition to building these teams, the bill will also authorize spending to bring in private companies when needed.

The new capabilities will be available to all public and private organizations on request, including businesses, hospitals, police departments, banks and educational establishments such as schools and colleges. The teams' responsibilities will involve assisting organizations in recovering from attacks and outages, risk assessment and threat mitigation, and developing recommendations for network best practices and data security at numerous DHS offices.

The new law shows that steps are being taken towards improving awareness amongst organizations regarding the impact of a ransomware cyber-attack. Additionally, it demonstrates that the government is acknowledging the importance of protecting businesses against cyber-attacks, including reducing cyber security risks and the downtime many organizations suffer as a result.

Furthermore, while improving the recovery time from a ransomware attack and mitigating threats should be a priority, the focus will also be on protecting and encrypting data. The technology is there for organizations to adopt, but many companies still believe their data is safe when it is not, which is what cybercriminals are counting on.

By encrypting sensitive data, defining a strong security policy, and implementing Observability tools that truly provide contextual data insights, organizations have a greater chance of troubleshooting and detecting a potential infiltration much earlier. The DHS Cyber Hunt and Incident Response Teams Act is certainly necessary in bringing cybersecurity to the forefront and in providing the assistance organizations need in order to design and implement effective security strategy .

Contact Certes Networks

300 Corporate Center Drive, Suite140
Pittsburgh, PA15108

Tel: 1(888)833-1142
Fax: 1(412)262-2574

info@certesnetworks.com
sales@certesnetworks.com

We offer an encryption solution that is simple, scalable and uncomplicated.