August 21, 2019

CISA INSIGHTS

Ransomware Outbreak

The Threat and How to Think About It

Ransomware has rapidly emerged as the most visible cybersecurity risk playing out across our nation's networks, locking up private sector organizations and government agencies alike. And that's only what we're seeing – many more infections are going unreported, ransoms are being paid, and the vicious ransomware cycle continues on. We strongly urge you to consider ransomware infections as destructive attacks, not an event where you can simply pay off the bad guys and regain control of your network (do you really trust a cybercriminal?).

CISA's Role as the Nation's Risk Advisor

Helping organizations protect themselves from ransomware attacks is a chief priority for the Cybersecurity and Infrastructure Security Agency (CISA). We have assisted many ransomware response and recovery efforts, building an understanding of how ransomware attacks unfold, and what potential steps you can take to better defend systems. But we also recognize that there's no such thing as perfect cybersecurity and ransomware infections can still happen, so we've also developed recommendations to help organizations limit damage, and recover smartly and effectively.

Ransomware Mitigations to Help You Defend Today and Secure Tomorrow

The below recommendations – our first "CISA INSIGHTS" product – lay out three sets of straightforward steps any organization can take to manage their risk. These recommendations are written broadly for all levels within an organization. It's never as easy as it should be, so if you need help, we urge you to reach out for assistance – CISA is here to help, but so is the FBI, numerous private sector security firms, state authorities, and others.

Actions for Today – Make Sure You're Not Tomorrow's Headline:

1. Backup your data, system images, and configurations and keep the backups offline
2. Update and patch systems
3. Make sure your security solutions are up to date
4. Review and exercise your incident response plan
5. Pay attention to ransomware events and apply lessons learned

Actions to Recover If Impacted – Don't Let a Bad Day Get Worse:

1. Ask for help! Contact CISA, the FBI, or the Secret Service
2. Work with an experienced advisor to help recover from a cyber attack
3. Isolate the infected systems and phase your return to operations
4. Review the connections of any business relationships (customers, partners, vendors) that touch your network
5. Apply business impact assessment findings to prioritize recovery

Actions to Secure Your Environment Going Forward – Don't Let Yourself be an Easy Mark:

1. Practice good cyber hygiene; backup, update, whitelist apps, limit privilege, and use multifactor authentication
2. Segment your networks; make it hard for the bad guy to move around and infect multiple systems
3. Develop containment strategies; if bad guys get in, make it hard for them to get stuff out
4. Know your system's baseline for recovery
5. Review disaster recovery procedures and validate goals with executives

Please visit the CISA Resource Page on Ransomware for more information. Victims of ransomware should report it immediately to CISA at www.us-cert.gov/report, a local FBI Field Office, or Secret Service Field Office.