WEST VIRGINIA INSURANCE BULLETIN
No. 21 - 05

Insurance Bulletins are issued when the Commissioner renders formal opinions, guidance or expectations on matters or issues, explains how new statutes or rules will be implemented or applied, or advises of interpretation or application of existing statutes or rules.

► Cybersecurity Alert ◄

In January 2021, the Cybersecurity and Infrastructure Security Agency (CISA) announced the *Reduce the Risk of Ransomware Campaign*, a focused, coordinated and sustained effort to encourage public and private sector organizations to implement best practices, tools and resources that can help them mitigate the cybersecurity risk and threat. As cybercrime becomes more common and costly, cyber risk continues to increase for all organizations. The COVID-19 pandemic has shifted more of our work and lives online. This shift has introduced new vulnerabilities that cybercriminals are aggressively exploiting. From the rise of ransomware to the recent JBS S.A. and Colonial Pipeline cyberattack campaigns, cybersecurity is now critically important to almost every aspect of modern life including consumer protection to national security.

To increase awareness to ever-growing cybersecurity threats, the West Virginia Offices of the Insurance Commissioner is issuing this **Cybersecurity Alert** on ransomware.

What is Ransomware?

According to the U.S. Computer Emergency Readiness Team ("US-CERT"), ransomware is a specific type of malicious program (i.e., a virus) where the victim's computer, network, and/or files become strongly encrypted to the point they are effectively rendered useless. Shortly after the victim realizes what happened, the victim typically receives a message demanding a ransom in exchange for restoring access to the affected systems. The number and size of ransomware incidents have increased significantly and strengthening our resilience from cyberattacks, in both private and public sectors, is a critical responsibility.

How is Ransomware Spread?

According to US-CERT, ransomware can be spread through e-mails that contain the malicious program or contain links to an infected website, or through messages or links sent through social media; however, in some recent variants, ransomware is spread by means of a "drive-by download attack," which occurs when an attacker covertly "injects" an ordinary website – usually a trusted or popular website – with malicious code, which, in turn, is downloaded and installed on unsuspecting visitors' computers.

Potential Impact

All organizations, both private and public, must recognize that no entity, employer, or employee is safe from being targeted by ransomware, regardless of size or location. According to the FBI, victims have included hospitals, school districts, state and local governments, and law enforcement agencies. In short, anyone with a computer and internet access could potentially become the next victim of a ransomware attack.

Possible Solutions

CISA lists several mitigation strategies[1] to help reduce the risk of a ransomware attack, including:

- ***Require multi-factor authentication*** *for remote access to OT and IT networks.*
- ***Enable strong spam filters to prevent phishing emails from reaching end users****. Filter emails containing executable files from reaching end users.*
- ***Implement a user training program and simulated attacks for spearphishing*** *to discourage users from visiting malicious websites or opening malicious attachments and re-enforce the appropriate user responses to spearphishing emails.*
- ***Filter network traffic*** *to prohibit ingress and egress communications with known malicious IP addresses. Prevent users from accessing malicious websites by implementing URL blocklists and/or allow lists.*
- ***Update software****, including operating systems, applications, and firmware on IT network assets, in a timely manner. Consider using a centralized patch management system; use a risk-based assessment strategy to determine which OT network assets and zones should participate in the patch management program.*
- ***Limit access to resources over networks, especially by restricting access****. After assessing risks, if RDP is deemed operationally necessary, restrict the originating sources and require multi-factor authentication.*
- ***Set antivirus/antimalware programs to conduct regular scans*** *of IT network assets using up-to-date signatures. Use a risk-based asset inventory strategy to determine how OT network assets are identified and evaluated for the presence of malware.*
- ***Implement unauthorized execution prevention by****:*
    - ***Disabling macro scripts from Microsoft Office files*** *transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full Microsoft Office suite applications.*
    - ***Implementing application allowlisting****, which only allows systems to execute programs known and permitted by security policy. Implement software restriction policies (SRPs) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.*
    - ***Monitor and/or block inbound connections from Tor exit nodes and other anonymization services*** *to IP addresses and ports for which external connections are not expected (i.e., other than VPN gateways, mail ports, web ports). For more guidance, refer to Joint Cybersecurity Advisory AA20-183A: Defending Against Malicious Cyber Activity Originating from Tor.*

[1] Alert (AA21-131A) DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks.

- ***Deploy signatures to detect and/or block inbound connection from Cobalt Strike servers*** *and other post exploitation tools.*

Ransomware attacks have disrupted organizations around the world, from hospitals across Ireland, Germany and France, to pipelines in the United States and banks in the U.K. The threats are serious, and they are increasing. We urge you to convene with your leadership teams to discuss the ransomware threat and review corporate security and business continuity plans to ensure you can continue or quickly restore operations.

Additional CISA Resources can be found at: https://www.cisa.gov/ransomware. Please e-mail any questions concerning this Insurance Bulletin to OICBulletins@wv.gov or call (304) 558-0401.

Issued: June 24, 2021

State of West Virginia
INSURANCE COMMISSIONER
Office of the Insurance Commissioner