REFERENCE GUIDE

DRAGOS

SEPTEMBER 2022

MeriTalk

CISA'S SHIELDS UP
QUICK REFERENCE GUIDE

Following the Russian invasion of Ukraine, the Cybersecurity and Infrastructure Security Agency (CISA) announced a warning to all U.S. organizations to keep their "shields up" in anticipation of malicious Russian cyber activity. Among troves of guidance, what is the bottom line?

ACTION ITEMS FOR ALL ORGANIZATIONS [1]

Ben Miller, Dragos VP of Services

> "Agencies with OT/ICS environments are often in the very early stages of their OT cybersecurity journey. There's a lot of complexity, as more and more devices become interconnected and interdependent. The threat is real, but the defense can get ahead of the challenge, and ShieldsUp has helped to amplify the challenges of our constantly evolving cybersecurity landscape."

REDUCE RISK

- Enforce multi-factor authentication (MFA)
- Disable non-essential ports and protocols
- Update software; check for vulnerabilities
- Use CISA's cyber hygiene services

▸ Strengthen cloud practices:

- Implement conditional access policies
- Establish baseline for normal activity
- Actively review for anomalous activity
- Focus on staff awareness and training
- Establish blame-free employee reporting[2]

▸ Regularly review/monitor:

- Active directory sign-ons and unified audit logs
- User-created email forwarding, rules, and alerts[3]

DETECT RISK

- ID and assess unusual network behavior
- Enable logging
- Use antivirus/antimalware software everywhere and keep up to date

IF WORKING WITH UKRAINIAN ORGANIZATIONS, TAKE EXTRA CARE

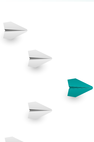
RESPOND TO RISK

- Designate a crisis-response team
- Assure availability of key personnel and surge support
- Define incident and roles/responsibilities
- Practice with a tabletop exercise

MAXIMIZE RESILIENCE:

- Test backup procedures
- Test manual controls

LESSONS FOR LEADERSHIP



- Empower Chief Information Security Officers (CISO)
- Lower reporting thresholds
- Participate in response plan testing
- Consult CISA's Ransomware Response Checklist[3]
- Focus on continuity of vital work
- Plan for the worst-case scenario

Report anomalous cyber activity and/or cyber incidents 24/7 to report@cisa.gov or (888) 282-0870

[1] CISA Shields Up
[2]Strengthening Security Configurations to Defend Against Attackers Targeting Cloud Services
[3]CISA Ransomware Guide

MeriTalk

DRAGOS

www.dragos.com