March 2, 2022

Workiva's response to Russia's attack on the Ukraine: Volatile times call for heightened cybersecurity preparedness.

Workiva closely follows the guidelines published by the U.S. Cybersecurity & Infrastructure Security Agency's (CISO) SHIELDS UP initiative, and guidance from the European Union Agency for Cybersecurity (ENISA) and has committed to sharing any incidents or anomalous activity to the proper law enforcement authorities in the jurisdiction(s) where the activity occurs.

Workiva has implemented ENISA and CERT-EU set of recommendations:

1. Ensure remotely accessible services require multi-factor authentication (MFA).

- Workiva requires all Workiva constituents to use Single Sign On with Multi Factor Authentication. Workiva recommends our customers to implement Single Sign On.

2. Ensure users do not re-use passwords, encourage users to use Multiple Factor Authentication (MFA) whenever supported by an application (on social media for instance).

- Workiva requires a complex password in addition to our Single Sign On and Multi Factor Authentication. We recommend customers set passwords in line with their internal policies and implement Single Sign On as well.

3. Ensure all software is up-to-date.

- Workiva utilizes automated patching mechanisms to ensure that host and container software is patched and up to date. Vulnerabilities identified in 3rd-party libraries included in our application are prioritized by severity and patched as part of our SDLC.

4. Tightly control third party access to your internal networks and systems.

- All Workiva access is based on least privileged and requires the use of unique IDs with adherence to our password policies. Access must be approved by the functional manager and system owner as managed through our ticketing system. All activity within Workiva's network and systems are logged to our centralized SIEM tool.

5. Pay special attention to hardening your cloud environments before moving critical loads to the Cloud.

- Workiva has established and documented our configuration settings in line with Center for Internet Security (CIS) baselines and SCAP compliant checklists.

6. Review your data backup strategy.

- Workiva utilizes redundant data backup in order to provide point-in-time recovery. In addition, Workiva allows customers to self-administer their accounts. At any time, a customer can save/export a document or delete a document. Workiva supports saving files in DOCX (MS Word), XLSX (MS Excel), or PDF (Adobe) formats for archiving on their own systems. Workiva also supports exporting in XML format for later use within the platform.

- Customer Tools: https://support.workiva.com/hc/en-us/articles/360035639692-Prepare-for-the-Unexpected

7. Change all default credentials and disable protocols that do not support multi-factor authentication or use weak authentication (e.g. cleartext passwords, or outdated and vulnerable authentication or encryption protocol

- Workiva has established and documented our configuration settings in line with Center for Internet Security (CIS) baselines and SCAP compliant checklists. Workiva requires all Workiva constituents to use Single Sign On with Multi Factor Authentication. Workiva recommends our customers to implement Single Sign On.

8. Employ appropriate network segmentation and restrictions to limit access and utilise additional attributes (such as device information, environment, and access paths) when making access decisions.

- Workiva prohibits the use of shared user IDs and all system access is logged.
- All administrative tasks are captured in our ticketing system and are governed by our change control process within our Information Security Policies. System logs from cloud providers are aggregated into our centralized SIEM. All access is granted through our single sign on, which requires multi-factor authentication that is FIPS-140-2 validated. Device trust is managed and controlled through device-specific requirements and locations.

9. Conduct regular training to ensure that IT and system administrators have a solid understanding of your organisation's security policy and associated procedures.

- Workiva employees receive regular security awareness training around policies, procedures, and processes on an annual basis based on their role and access.

10. Create a resilient email security environment by enabling antispam filtering, adding a secure email gateway configured to automatically follow field-tested policies and playbooks designed to prevent malicious emails from reaching mailboxes.

- Workiva utilizes email spam filtering and blocks any automatic forwarding of emails, additionally devices and servers run anti-malware tooling.

11. Organize regular cyber awareness events to train your users on common phishing techniques (e.g. identifying spoofed/suspicious messages) and the effects of phishing attacks.

- Workiva employees undergo various security awareness and other training on at least an annual basis. Additionally, Workiva performs social engineering campaigns on a regular basis. Where needed, additional training is provided.

12. Protect your web assets from denial-of-service attacks.

- Workiva's platform is based on the AWS cloud platform and benefits directly from AWS' managed DDoS Protection service, AWS Shield.

13. Block or severely limit internet access for servers or other devices that are seldom rebooted, as they are coveted by threat actors for establishing backdoors and creating persistent beacons to Command and Control (C2) infrastructure.

- Workiva infrastructure operates in a "servers as commodities" environment, servers are short lived and managed by configuration as code to ensure they cannot be modified.

14. Make sure you have the procedures to reach out and swiftly communicate with your CSIRT.

- Workiva maintains an incident response plan with contact details for the relevant authorities in jurisdictions where we operate.

Additional Resources

- CISA Insights: Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure (pdf) (February 2022)
- CISA Insights: Implement Cybersecurity Measures Now to Protect Against Potential Critical Threats (pdf) (January 2022)
- Alert (AA22-011A) Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure (January 2022)
- CISA Insights: Preparing For and Mitigating Potential Cyber Threats (pdf) (December 2021)
- Reminder for Critical Infrastructure to Stay Vigilant Against Threats During Holidays and Weekends (November 2021)
- COVID-19 Disinformation Toolkit
- Mis-, Dis-, and Malinformation (MDM) Planning and Incident Response Guide for Election Officials
- MDM Rumor Control Page Start-Up Guide
- Russia Cyber Threat Overview and Advisories
- Free Public and Private Sector Cybersecurity Tools and Services
- War on Pineapple
- External Resources
- RESIST 2 Counter Disinformation Toolkit - GCS (civilservice.gov.uk)

- **Swedish Civil Contingencies Agency (MSB) | Countering Disinformation**