 

2 de março de 2022

Resposta da Workiva ao ataque da Rússia à Ucrânia: Tempos voláteis exigem maior atenção

preparação para a segurança cibernética.

A Workiva segue rigorosamente as diretrizes publicadas pelo U.S. Cybersecurity & Infrastructure

A CISO (Security Agency) a [,iniciativa SHIELDS UP](https://www.cisa.gov/shields-up) e ENISA ([a orientação da European Union Agency](https://www.enisa.europa.eu/publications/boosting-your-organisations-cyber-resilience)  [for Cybersecurity](https://www.enisa.europa.eu/publications/boosting-your-organisations-cyber-resilience)) e se comprometeu a compartilhar quaisquer incidentes ou atividades anômalas com as autoridades competentes da aplicação da lei na(s) jurisdição(ões) onde a atividade ocorre.

A Workiva implementou o conjunto de recomendações da ENISA e do CERT-EU:

1. **Garanta que os serviços de acesso remoto exijam autenticação multifator (MFA).**
	* A Workiva exige que todos os constituintes da Workiva usem o Single Sign On com Multi Factor Authentication. A Workiva recomenda que nossos clientes implementem o Single Sign On.
2. **Certifique-se de que os usuários não reutilizem as senhas e incentive-os a usar a autenticação de múltiplos fatores (MFA) sempre que suportada por um aplicativo (nas mídias sociais, por exemplo).**
	* A Workiva exige uma senha complexa, além de nosso Single Sign On e Multi Factor Authentication. Recomendamos que os clientes definam senhas de acordo com suas políticas internas e implementem o Single Sign On também.
3. **Certifique-se de que todos os softwares estejam atualizados.**
	* A Workiva utiliza mecanismos automatizados de aplicação de patches para garantir que o software do host e do contêiner seja corrigido e atualizado. As vulnerabilidades identificadas em bibliotecas de terceiros incluídas em nosso aplicativo são priorizadas por gravidade e corrigidas como parte de nosso SDLC.
4. **Controle rigorosamente o acesso de terceiros às suas redes e sistemas internos.**
	* Todo o acesso à Workiva é baseado em privilégios mínimos e requer o uso de IDs exclusivos com adesão às nossas políticas de senha. O acesso deve ser aprovado pelo gerente funcional e pelo proprietário do sistema, conforme gerenciado por meio de nosso sistema de tíquetes. Todas as atividades na rede e nos sistemas da Workiva são registradas em nossa ferramenta SIEM centralizada.
5. **Preste atenção especial à proteção de seus ambientes de nuvem antes de mover cargas críticas para a nuvem.**
	* A Workiva estabeleceu e documentou nossas definições de configuração de acordo com as linhas de base do Center for Internet Security (CIS) e as listas de verificação em conformidade com o SCAP.
6. **Revise sua estratégia de backup de dados.**
	* A Workiva utiliza backup redundante de dados para oferecer recuperação pontual. Além disso, a Workiva permite que os clientes administrem suas contas por conta própria. A qualquer momento, um cliente pode salvar/exportar um documento ou excluir um documento. A Workiva suporta o salvamento de arquivos nos formatos DOCX (MS Word), XLSX (MS Excel) ou PDF (Adobe) para arquivamento em seus próprios sistemas. A Workiva também suporta a exportação em formato XML para uso posterior na plataforma.
	* Ferramentas do cliente [:https://support.workiva.com/hc/en-us/articles/360035639692-](https://support.workiva.com/hc/en-us/articles/360035639692-Prepare-for-the-Unexpected)  [Prepare-se para o inesperado](https://support.workiva.com/hc/en-us/articles/360035639692-Prepare-for-the-Unexpected)
7. **Altere todas as credenciais padrão e desative os protocolos que não oferecem suporte à autenticação multifatorial ou que usam autenticação fraca (por exemplo, senhas de texto não criptografado ou protocolo de autenticação ou criptografia desatualizado e vulnerável)**
	* A Workiva estabeleceu e documentou nossas definições de configuração de acordo com as linhas de base do Center for Internet Security (CIS) e as listas de verificação compatíveis com SCAP. A Workiva exige que todos os constituintes da Workiva usem o Single Sign On com Multi Factor Authentication. A Workiva recomenda que nossos clientes implementem o Single Sign On.
8. **Empregar segmentação e restrições de rede adequadas para limitar o acesso e utilizar atributos adicionais (como informações do dispositivo, ambiente e caminhos de acesso) ao tomar decisões de acesso.**
	* A Workiva proíbe o uso de IDs de usuário compartilhados e todos os acessos ao sistema são registrados.
	* Todas as tarefas administrativas são capturadas em nosso sistema de emissão de tíquetes e são regidas por nosso processo de controle de alterações dentro de nossas Políticas de Segurança da Informação. Os registros do sistema dos provedores de nuvem são agregados ao nosso SIEM centralizado. Todo o acesso é concedido por meio de nosso logon único, que exige autenticação multifatorial validada pelo FIPS-140-2. A confiança do dispositivo é gerenciada e controlada por meio de requisitos e locais específicos do dispositivo.
9. **Realizar treinamentos regulares para garantir que os administradores de TI e de sistemas tenham uma sólida**

**compreensão da política de segurança de sua organização e dos procedimentos associados.**

* + Os funcionários da Workiva recebem treinamento regular de conscientização de segurança sobre políticas, procedimentos e processos anualmente, com base em sua função e acesso.
1. **Crie um ambiente de segurança de e-mail resiliente ativando a filtragem antispam, adicionando um gateway de e-mail seguro configurado para seguir automaticamente políticas testadas em campo e manuais projetados para impedir que e-mails mal-intencionados cheguem às caixas de correio.**
	* A Workiva utiliza filtragem de spam de e-mail e bloqueia qualquer encaminhamento automático de e-mails. Além disso, os dispositivos e servidores executam ferramentas antimalware.
2. **Organize eventos regulares de conscientização cibernética para treinar seus usuários sobre técnicas comuns de phishing (por exemplo, identificar mensagens falsas/suspeitas) e os efeitos dos ataques de phishing.**
	* Os funcionários da Workiva passam por vários treinamentos de conscientização de segurança e outros treinamentos pelo menos uma vez por ano. Além disso, a Workiva realiza campanhas de engenharia social regularmente. Quando necessário, é fornecido treinamento adicional.
3. **Proteja seus ativos da Web contra ataques de negação de serviço.**
	* A plataforma da Workiva se baseia na plataforma de nuvem da AWS e se beneficia diretamente dos recursos da AWS

serviço gerenciado de proteção contra DDoS, o AWS Shield.

1. **Bloqueie ou limite severamente o acesso à Internet para servidores ou outros dispositivos que raramente são reinicializados, pois eles são cobiçados por agentes de ameaças para estabelecer backdoors e criar beacons persistentes para a infraestrutura de Comando e Controle (C2).**
	* A infraestrutura da Workiva opera em um ambiente de "servidores como commodities", os servidores são

de curta duração e gerenciados por configuração como código para garantir que não possam ser modificados.

1. **Certifique-se de que você tenha os procedimentos para entrar em contato e se comunicar rapidamente com o CSIRT.**
	* A Workiva mantém um plano de resposta a incidentes com detalhes de contato para as autoridades relevantes nas jurisdições em que opera.

**Recursos adicionais**

* + [**Insights da CISA: Preparing for and Mitigating Foreign Influence Operations Targeting**](https://www.cisa.gov/sites/default/files/publications/cisa_insight_mitigating_foreign_influence_508.pdf)[**Critical Infrastructure**](https://www.cisa.gov/sites/default/files/publications/cisa_insight_mitigating_foreign_influence_508.pdf) **(pdf) (fevereiro de 2022)**
	+ [**Insights da CISA: Implemente medidas de segurança cibernética agora para se proteger contra possíveis**](https://www.cisa.gov/sites/default/files/publications/CISA_Insights-Implement_Cybersecurity_Measures_Now_to_Protect_Against_Critical_Threats_508C.pdf)[**ameaças críticas**](https://www.cisa.gov/sites/default/files/publications/CISA_Insights-Implement_Cybersecurity_Measures_Now_to_Protect_Against_Critical_Threats_508C.pdf) **(pdf) (janeiro de 2022)**
	+ [**Alerta (AA22-011A) Entendendo e mitigandocibernéticas patrocinadas pelo Estado russoas ameaçasà infraestrutura crítica dos EUA**](https://www.cisa.gov/uscert/ncas/alerts/aa22-011a) **(janeiro de 2022)**
	+ [**Insights da CISA: Preparando-se e mitigando possíveis ameaças cibernéticas**](https://www.cisa.gov/sites/default/files/publications/CISA_INSIGHTS-Preparing_For_and_Mitigating_Potential_Cyber_Threats-508C.pdf) **(pdf) (dezembro de 2021)**
	+ [**Lembrete para que a infraestrutura crítica permaneça vigilante contra ameaças durante feriados e**](https://www.cisa.gov/uscert/ncas/current-activity/2021/11/22/reminder-critical-infrastructure-stay-vigilant-against-threats) **fins** [**de semana**](https://www.cisa.gov/uscert/ncas/current-activity/2021/11/22/reminder-critical-infrastructure-stay-vigilant-against-threats) **(novembro de 2021)**
	+ [**Kit de ferramentas de desinformação sobre a COVID-19**](https://www.cisa.gov/publication/covid-19-disinformation-toolkit)
	+ [**autoridadesGuia de planejamento e resposta a incidentes de desinformação, desinformação e malinformação (MDM) paraeleitorais**](https://www.cisa.gov/sites/default/files/publications/mdm-incident-response-guide_508.pdf)
	+ [**Guia de inicialização da página de controle de rumores do MDM**](https://www.cisa.gov/sites/default/files/publications/rumor-control-startup-guide_508.pdf)
	+ [**Visão geral e avisos sobre ameaças cibernéticas na Rússia**](https://www.cisa.gov/uscert/russia)
	+ [**Ferramentas e serviços gratuitos de segurança cibernética para os setores público e privado**](https://www.cisa.gov/free-cybersecurity-tools-and-services)
	+ [**Guerra ao abacaxi**](https://www.cisa.gov/publication/war-pineapple)
	+ **Recursos externos**
	+ [**Kit de ferramentas de combate à desinformação RESIST 2 - GCS (civilservice.gov.uk)**](https://gcs.civilservice.gov.uk/publications/resist-2-counter-disinformation-toolkit/)
	+ [**Agência Sueca de Contingências Civis (MSB) | Combate à desinformação**](https://counteringdisinformation.org/taxonomy/term/822)