TLP:GREEN

Livre compartilhamento

RECOMENDAÇÕES

Atualizações de Equipamentos e Sistemas Operacionais

#003 - Priorização das ações de atualização de equipamentos e sistemas operacionais

Diante do atual contexto de transição e evolução nas práticas governamentais, torna-se relevante adotar abordagens diferenciadas para mitigar os possíveis riscos cibernéticos e garantir a contínua operabilidade dos sistemas e serviços fundamentais para a sociedade. Por diversas razões, muitos sistemas e equipamentos EOSL (*End of Service Life*) ainda estão em plena operação em vários ambientes, o que demanda dos gestores uma atenção especial para manter a segurança das operações. Esses sistemas EOSL ativos podem facilmente se tornar alvo de ataques por parte de atores mal-intencionados, isso aumenta o perfil de risco cibernético que a instituição precisa lidar.

Nesse sentido, esta recomendação apresenta um conjunto de medidas a serem implementadas quanto à segurança para sistemas operacionais Microsoft EOSL, elaborado pelo Centro Integrado de Segurança Cibernética do GOV.BR (CISC GOV.BR), destacando a importância das instituições priorizarem o uso de equipamentos e sistemas operacionais atualizados e com suporte do fabricante. Tais medidas são consideradas emergenciais e transitórias, visando reduzir prontamente os níveis de exposição a potenciais ameaças cibernéticas decorrentes da utilização de soluções desatualizadas.

Como informação e base norteadora, a tabela abaixo apresenta os sistemas operacionais Microsoft e a respectiva data de término do suporte.

MICROSOFT WINDOWS *SUPPORT END OF LIFE*

Versão do Windows	Data de Término do Suporte
Windows 95	31 de dezembro de 2001
Windows 98	11 de julho de 2006
Windows ME	11 de julho de 2006
Windows 2000	13 de julho de 2010
Windows XP	8 de abril de 2014
Windows Server 2003	14 de julho de 2015
Windows Vista	11 de abril de 2017
Windows 7	14 de janeiro de 2020
Windows Server 2008	14 de janeiro de 2020
Windows Server 2008 R2	14 de janeiro de 2020
Windows 8	12 de janeiro de 2016
Windows 8.1	10 de janeiro de 2023
Windows Server 2012	10 de outubro de 2023
Windows Server 2012 R2	10 de outubro de 2023
Windows 10 (versão 1507)	9 de maio de 2017
Windows 10 (versão 1511)	10 de outubro de 2017
Windows 10 (versão 1607)	10 de abril de 2018
Windows 10 (versão 1703)	9 de outubro de 2018
Windows 10 (versão 1709)	9 de abril de 2019
Windows 10 (versão 1803)	12 de novembro de 2019
Windows 10 (versão 1809)	12 de novembro de 2019
Windows 10 (versão 1903)	8 de dezembro de 2020
Windows 10 (versão 1909)	11 de maio de 2021
Windows 10 (versão 2004)	14 de dezembro de 2021

Tabela 1

O CISC GOV.BR recomenda a implementação das seguintes medidas de controle emergenciais para reduzir o nível de risco associado aos sistemas EOSL e, consequentemente, fortalecer a segurança do ambiente.

Medida 1 - Avaliação de Risco

Hipótese 01: Identificar os sistemas operacionais sem suporte em uso na organização.

Prática Recomendada: Avaliar o risco associado a esses sistemas, considerando fatores como a exposição à internet, dados críticos armazenados e a importância desses sistemas para as operações.

Medida 2 - Isolamento e Segmentação

Hipótese 02: Isolar os sistemas sem suporte em uma rede separada.

Prática Recomendada: Controlar o acesso a essa rede partir de outros segmentos da rede.

Segmentar esses sistemas em uma VLAN dedicada para reduzir o impacto caso ocorra uma exploração.

Medida 3 - Monitoramento Contínuo

Hipótese 03: Implementar monitoramento de segurança para detectar atividades suspeitas ou tentativas de exploração.

Práticas Recomendada: Utilizar ferramentas de detecção de intrusão e registrar eventos relevantes.

Medida 4 - Mitigação de Vulnerabilidades

Hipótese 04: Manter os sistemas operacionais sem suporte atualizados com as últimas correções de segurança disponíveis.

Prática Recomendada: Implementar soluções de segurança, como firewalls, antivírus e sistemas de prevenção de intrusão, criando regras específicas para alertas e ações para equipamentos e sistemas legados.

Medida 5 - Plano de Resposta a Incidentes

Hipótese 05: Desenvolver um plano de resposta específico para sistemas sem suporte.

Prática Recomendada: Incluir procedimentos para isolar sistemas comprometidos, notificar partes interessadas e restaurar serviços.

Medida 6 - Comunicação Interna e Treinamento

Hipótese 06: Treinar os colaboradores sobre os riscos associados aos sistemas sem suporte.

Prática Recomendada: Comunicar as diretrizes e procedimentos relevantes para toda a equipe.

Medida 7 - Comunicação Interna e Treinamento:

Hipótese 07: Treinar os colaboradores sobre os riscos associados aos sistemas sem suporte.

Prática Recomendada: Comunicar as diretrizes e procedimentos relevantes para toda a equipe.

DOCUMENTOS DE APOIO

1. **Guia de Resposta a Incidentes**

https://www.gov.br/governodigital/pt-br/privacidade-eseguranca/ppsi/guia_resposta_incidentes.pdf

2.**Guia de Gerenciamento de Vulnerabilidades** https://www.gov.br/governodigital/pt-br/privacidade-eseguranca/ppsi/guia_gerenciamento_vulnerabilidades.pdf

3.**Framework de Privacidade e Segurança da Informação**

https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_framework_psi.pdf

REFERÊNCIAS

1. Fim do suporte para o Windows Server e Aplicativos do Microsoft 365

https://learn.microsoft.com/pt-br/deployoffice/endofsupport/windows-server-support

2. Fim do suporte para Windows 10, Windows 8.1 e Windows 7

https://www.microsoft.com/pt-br/windows/end-of-support

3. Guia Essencial para Gestão de Vulnerabilidades:

https://br.startupdefense.io/blog/o-guia-essencial-para-gestao-de-vulnerabilidades

4. Red Hat - O que é Gerenciamento de Vulnerabilidades?

https://www.redhat.com/pt-br/topics/security/what-is-vulnerability-management

5. ServiceNow - Vulnerability Response:

https://www.servicenow.com/br/products/vulnerability-response.html