Recomendação de Segurança 004/2021 - Cogetic

Em 1º de julho de 2021

Para: VPEIC, Áreas de TI correlatas e anfitriões de em reuniões através da ferramenta Zoom

Assunto: Recomendações de segurança para configuração do aplicativo Zoom

Prezados Gestores de TI,

O *Zoom Meeting (Reuniões Zoom)* é uma ferramenta bastante utilizada pelo mercado para a realização de reuniões. Diante do cenário global de ameaças digitais frente a essa modalidade de aplicativo, estamos por meio desta, revisando o Recomendação de Segurança 001/2020, publicada em 8 de abril de 2020.

Recomendações de segurança (medidas para mitigação)

Listamos abaixo algumas recomendações de segurança para a utilização da ferramenta Zoom Meeting, cabendo ao anfitrião avaliar o cenário ideal, considerar os riscos envolvidos e aplicar as medidas adequadas conforme recomendações abaixo:

1. Todos os participantes devem dar preferência ao cliente web. Ao usar o aplicativo, devem usar instalador disponibilizado no site oficial do Zoom Meeting e garantir que estão com a última versão estável disponibilizada. É aconselhável que os participantes habilitem a autenticação de dois fatores para acesso as reuniões no aplicativo Zoom. Para isso o participante deve acessar o menu de navegação e clicar na opção ‘Avançado’ e, a seguir, clicar em ‘Segurança’. Ative a opção “entrar com autenticação de dois fatores”. Em complemento a esta ação baixar o aplicativo Microsoft Authenticator através do qual o participante receberá uma senha de uso único (OTP) sempre que desejar fazer login no Zoom. Ainda há outra opção caso o participante deseje emparelhar seu telefone, receberá uma senha de uso único (OTP) sempre que desejar fazer login no Zoom.

Habilitando 2FA (administrador-Anfitrião):

— Faça login no portal da web do Zoom.

— No menu de navegação, clique em Avançado e em Segurança.

— Certifique-se de que a opção Sign in with Two-Factor Authentication está habilitada.

— Selecione uma dessas opções para especificar os usuários para habilitar 2FA para:

— Todos os usuários em sua conta: Habilite 2FA para todos os usuários na conta.

— Usuários com funções específicas: Habilite 2FA para funções com as funções especificadas. Clique no ícone de lápis, selecione as funções e clique em OK.

— Usuários pertencentes a grupos específicos: Habilite 2FA para usuários que estão nos grupos especificados. Clique no ícone de lápis, selecione os grupos e clique em OK.

— Clique em Salvar.

Nota: Você pode compartilhar as instruções para configurar 2FA com seus usuários.

2. O anfitrião deve configurar opções de segurança no momento de agendar uma reunião, tais como:
   — Enviar links de convite diretamente a cada participante, pessoa a pessoa;
   — Evite compartilhar o link da conferência do Zoom em mídias e redes sociais;
   — Habilitar o recurso "*Sala de espera*", permitindo que o anfitrião identifique e admita o ingresso do participante individualmente, antes que entre na sala de reunião.
   — Desabilitar o recurso "*Senha incorporada no link de convite para ingresso com um clique*", garantindo que o participante entre manualmente com a senha da sala de reunião;
3. Antes do início da reunião, o anfitrião deve considerar as seguintes situações:
   — Desabilitar recurso "*Permitir que os participantes ingressem antes do anfitrião*", evitando comportamentos inadequados e impróprios, sem a supervisão do responsável pela sala;
   — Habilitar o recurso "*Silenciar todos os participantes quando ingressarem em uma reunião*", para que os participantes entrem com o microfone mutado;
   — Desabilitar o recurso "*Vídeo dos participantes*", evitando projeção de imagens e situações inadequadas e impróprias para a reunião;

- Habilitar o recurso "*Salvar bate-papos automaticamente*", registrando todas as mensagens para auditoria futura.
- Desabilitar o recurso "*Bate-papo privado*", evitando comportamentos inadequados e impróprios direcionado.
- Desabilitar o recurso "*Permitir que os participantes se renomeiem*", evitando textos inadequadas e impróprias para a reunião;
- Desabilitar o recurso "*Ocultar as imagens de perfil do participante em uma reunião*", evitando projeção de imagens inadequadas e impróprias para a reunião;
- Desabilitar o recurso "*Transferência de arquivo*", evitando disseminação de arquivos inadequados e impróprios para a reunião;
- Habilitar o recurso "*Compartilhamento de tela*", somente com a opção "*Apenas anfitrião*" selecionado, evitando projeção de imagens e situações inadequadas e impróprias para a reunião;
- Desativar o recurso "*Controle remoto*", evitando manipulação inadequada e imprópria ao computador do apresentador; e
- Desabilitar o recurso "*Anotação*"; evitando disseminação de textos inadequados e impróprios para a reunião.

4. O anfitrião deve considerar as seguintes configurações avançadas:
   - Utilizar critérios de segurança para criação de senha forte para sua conta de acesso;
   - Habilitar o recurso "*Requer que todas as reuniões estejam protegidas por uma opção de segurança*", garantindo que ao menos uma opção de segurança disponível esteja habilitada;
   - Habilitar o recurso "*Senha da reunião*" ou "*Solicitar uma senha ao agendar novas reuniões*", permitindo obter uma senha para o ingresso na reunião;
   - Habilitar o recurso "*Solicitar uma senha para reuniões instantâneas*", para garantir que todos os participantes ingressem na reunião por senha;
   - Habilitar o recurso "*Solicitar uma senha para a ID de reunião pessoal (PMI)*" e selecionar a opção "*Todas as reuniões que usam PMI*", para garantir que todos os participantes ingressem na reunião por senha;
   - Habilitar o recurso "*Requer uma senha para as reuniões que já foram agendadas*", garantindo que todas as reuniões tenham uma senha;

- Quando for necessário habilitar o recurso "*Anotação*", e selecionar a opção "*Somente o usuário que está compartilhando pode fazer anotações*";
- Habilitar o recurso "*Senha do ID de reunião pessoal (PMI)*" ou "*Solicitar uma senha para a ID de reunião pessoal (PMI)",* permitindo o uso do identificador pessoal da reunião;
- Habilitar o recurso "*Solicitar senha para que os participantes ingressem pelo telefone*", garantindo que todos os participantes entrem na sala por meio de senha; e
- Para transmissões ao vivo (*Live streaming*), habilitar o recurso "*Permitir transmissão ao vivo de reuniões*", e selecionar a plataforma utilizada (Facebook,Youtube ou outros).

5. Cabe ao anfitrião as atribuições abaixo, e deve considerar designar pelo menos mais um coanfitrião para:
   - Ajudar no controle das salas virtuais de espera e de reunião;
   - Conferir participantes, não admitindo estranhos;
   - Remover da reunião participante que seja inconveniente, indesejado e/ ou que esteja impedindo o desenvolvimento adequado da reunião; e
   - Bloquear a sala de reunião, quando todos os participantes estiverem presentes, evitando que pessoas não convidadas ingressem.
6. O apresentador deve compartilhar apenas a tela essencial para a apresentação, com o recurso de "*Portion of Screen*";
7. Todos os participantes devem proteger sua câmera fisicamente, com *post-its* ou bloqueadores próprios para câmeras, liberando somente quando necessário; e
8. Todos os participantes devem redobrar o cuidado com links e arquivos compartilhados.

Vale ainda ressaltar que a Fiocruz que disponibiliza outras ferramentas para conferência, entre eles o Microsoft Teams e serviço de web conferência da RNP.

Referências:

— https://blog.zoom.us/pt/which-zoom-security-features-are-best-for-your-industry/

— https://zoom.us/pt-pt/trust/security.html

— https://www.kaspersky.com.br/blog/zoom-security-ten-tips/14711/

— https://br.ccm.net/faq/49446-zoom-como-melhorar-a-seguranca-das-reunioes

— https://support.zoom.us/hc/en-us/articles/360038247071-Setting-up-and-using-two-factor-authentication-2FA-

Coordenação de Gestão de Tecnologia da Informação
Segurança da Informação e Comunicações