CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

“Informe sobre aplicaciones para videoconferencia”

05 de abril de 2020

División de Redes y Seguridad Informática.

Gobierno de Chile

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

APLICACIONES DE VIDEOCONFERENCIA PARA TRABAJO A DISTANCIA

I.- Presentación

El trabajo a distancia ofrece muchas ventajas, pero no está libre de riesgos de seguridad, especialmente si se trata de compartir información entre los miembros de un grupo de trabajo o de asegurar la privacidad de la reunión. Dado que no existe un medio tecnológico libre de estas amenazas y riesgos, el Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile, CSIRT, ha elaborado el presente documento en el que se entregan algunas sugerencias de que software utilizar y recomendaciones para que la información que se transmite, al realizar una teleconferencia, pueda desarrollarse de la manera más segura posible.

II.- Resumen ejecutivo

Los medios tecnológicos permiten el despliegue de múltiples herramientas para comunicarse a distancia entre grupos de personas, las que son muy útiles para entornos personales y empresariales; en particular en momentos que la presencia física se ve dificultada por las condiciones de emergencia sanitaria.

En este contexto, el trabajo a distancia aporta múltiples beneficios a funcionarios e instituciones pero también conlleva riesgos para la seguridad de la información personal e institucional. Es necesario, entonces, considerar un conjunto de criterios que van más allá que la facilidad de utilización y número de usuarios que soporta la plataforma elegida, más aún, si los participantes de dichas reuniones representan a Instituciones críticas o sensibles en la organización o coordinación del País o de la actual crisis sanitaria.

Este trabajo a distancia debe considerarse una extensión del trabajo realizado en las oficinas de la institución y, por tanto, su seguridad no debe ser inferior al nivel mínimo exigido en la institución misma, más aún si ha de tener en consideración que eventualmente pueden usarse para tratar temas relacionados con seguridad nacional o de un nivel de confidencialidad secreto.

Es necesario, por tanto, antes de definir qué herramienta tecnológica para teleconferencias utilizar o descartar en su respectivo servicio, frente a la innumerable cantidad de informaciones de seguridad comprobadas y no comprobadas que circulan por

internet , se debe verificar las condiciones de seguridad acordes al nivel de sensibilidad y confidencialidad de la información que se transmitirá por dicha herramienta, descartando aquellas que tengan bajos niveles de protección y resguardos en base a fuentes comprobadas.

En particular, CSIRT, no sugiere la prohibición de ninguna de las herramientas de teleconferencias más utilizadas actualmente, sino que por el contrario entrega lineamientos y recomendaciones de seguridad para que los servicios opten por cuales usar según sea el contexto de las autoridades involucradas o de los temas a tratar.

III.- Desarrollo

1. Mejores prácticas aceptadas internacionalmente sobre comunicación institucional

Desde un punto de vista de marco normativo existen las normas ISO27002 que establecen controles generales para la seguridad de la información en las comunicaciones institucionales, tanto de las instalaciones primarias como para aquellas remotas y su paso por redes públicas. Complementariamente se suma la norma ISO27010, que introduce directrices sobre la gestión de seguridad de la información para las comunicaciones inter-sectoriales e inter-organizacionales. Más concretamente dicha norma aporta orientación sobre del funcionamiento interno de la empresa, seguridad y comunicación entre el propio sector, entre sectores y con los gobiernos. Con esto se consigue proteger la infraestructura crítica, reconocer las circunstancias normales para satisfacer los requisitos jurídicos, reglamentarios y otras obligaciones contractuales.

Sobre esta base normativa es que surgen criterios mínimos que deben considerarse para utilizar o seleccionar las herramientas de trabajo colaborativo o teleconferencias adecuadas a la seguridad de la información institucional.

La herramienta que provea la teleconferencia debe, al menos, cumplir con los siguientes requerimientos de seguridad de la información:

- Encriptado de extremo a extremo, utilizando algoritmos de cifrado robustos (verificando que no se incluyan aquellos que ya se han descartado por haberse quebrado su seguridad). Al menos considerar AES-256 para las conferencias normales y algoritmos de rango superior para conferencias de nivel seguridad nacional.

- Encriptado de las contraseñas.
- Autenticación de los participantes, en lo posible con segundo factor de autenticación. En lo posible con servidores centrales que estén bajo control institucional. Si la solución utilizada se encuentra en la nube se deben tomar los resguardos para que las comunicaciones, conversaciones y documentos que se intercambian queden, de ser requerido, almacenados de manera segura (encriptada).
- Soporte de cumplimiento e integración con otras soluciones de ciberseguridad como Data Loss Prevention (DLP) por ejemplo, e integración con otras herramientas organizacionales que permitan interoperar las funciones y plataformas de productividad y de uso institucional.
- Opciones de seguridad para los administradores de la plataforma.
- Las comunicaciones en lo posible deben ofrecer trazabilidad para efectos de auditorías posteriores en cuanto a su utilización.
- Establecer las consideraciones requeridas para verificar que la información transmitida NO es almacenada por el proveedor, sin el consentimiento o gestión del administrador del servicio, y que no se tiene acceso por parte del mismo, a la información personal de los participantes.
- Los aplicativos deben en un entorno rico en dispositivos de múltiples sistemas operativos, ofrecer capacidad multiplataforma para maximizar la flexibilidad de uso.
- Todo aplicativo eventualmente puede tener vulnerabilidades, ya sea por su codificación propia como por la plataforma sobre la cual se instala. Por tanto, un factor relevante a considerar es el soporte profesional con el que cuenta y el respaldo de sus desarrolladores para garantizar estabilidad, continuidad y seguridad mientras duren los contratos o expectativas de utilización de la herramienta.
- Cada herramienta debe entonces ser evaluada también por sus vulnerabilidades que pueden finalmente afectar o comprometer la seguridad de la teleconferencia, de la información personal e institucional de los participantes, y los activos institucionales.
- Con estos criterios generales e debe realizar un proceso de verificación que permita seleccionar la herramienta óptima en funcionalidad y en seguridad para tomar las bondades del trabajo a distancia sin comprometer la seguridad de la información institucional.

2. Herramientas disponibles en el mercado, clasificadas según vulnerabilidades encontradas.

A continuación, se mencionan algunas herramientas conjuntamente con el detalle de las vulnerabilidades históricas encontradas y reportadas sobre la base de CVE:

a) **Hangouts,** presenta vulnerabilidades asociadas al sistema operativo Android que es su soporte principal. Esta versión es considerada para comunicaciones del tipo hogar. La versión empresarial de este proveedor se denomina "Google Hangout Meet".
b) **Jitsi**, presenta solo una vulnerabilidad CVE registrada en 2017[1].
c) **ooVoo**, presenta solo una vulnerabilidad CVE registrada en 2009[2].
d) **Zoom Meeting**, presenta 5 vulnerabilidades registradas como CVE que dé nos estar mitigadas en la versión utilizada pueden comprometer la seguridad de la información[3].
e) **GoToMeeting,** presenta solo una vulnerabilidad CVE registrada en 2014[4].
f) **Microsof Skype**, presenta 6 vulnerabilidades CVE en versiones anteriores o iguales a 2017[5].
g) **Microsoft Team,** no presenta vulnerabilidades CVE registradas a la fecha. Es un producto de rango empresarial para establecer teleconferencias y trabajo colaborativo.
h) **Webex,** presenta 9 vulnerabilidades CVE registradas para versiones anteriores o iguales a 2017[6]

- A la fecha, no existen herramientas sin vulnerabilidades, en todos los softwares han existido y en todas ellas se han subsanados.
- No hay vigentes vulnerabilidades críticas que no hayan sido subsanadas.
- De existir nuevas vulnerabilidades, en las principales herramientas utilizadas, siempre hay empresas con rápidos tiempos de respuesta para subsanarlas y sacar nuevas versiones seguras.

3. Herramientas más usadas disponibles en el mercado.

Como se explicó en puntos anteriores, dependiendo de los niveles de sensibilidad de la información a poner sobre la plataforma, el número de usuarios, los niveles de autenticación, facilidad de uso y herramientas de control para la administración segura de la misma con servidores locales o en la nube, podemos recomendar las siguientes herramientas:

[1] https://www.cvedetails.com/vendor/16088/Jitsi.html

[2] https://www.cvedetails.com/product/16551/Oovoo-Oovoo.html?vendor_id=9335

[3] https://www.cvedetails.com/vulnerability-list/vendor_id-2159/Zoom.html

[4] https://www.cvedetails.com/product/26987/Citrix-Gotomeeting.html?vendor_id=422

[5] https://www.cvedetails.com/product/35646/Microsoft-Skype.html?vendor_id=26

[6] https://www.cvedetails.com/product/18500/Cisco-Webex.html?vendor_id=16

- BlueJeans
- Cisco Webex
- Google Hangout Meet
- Microsoft Team
- Microsoft Skype
- Pexip
- Zoom Meetings

Cada uno debe ser evaluado en su mérito y en cumplimiento de las políticas y normativas institucionales sobre seguridad de la información, uso de plataformas de teleconferencia sobre redes públicas no seguras, y el uso adicional de servicios en la nube (administración de la plataforma, almacenamiento de las comunicaciones grabadas, entre otros).

En complemento a este planteamiento se muestra el Cuadrante Mágico de Gartner con los principales actores según su posicionamiento (Leaders, Challenger, Visionaries o Niche Players). Ver Ilustración 1.

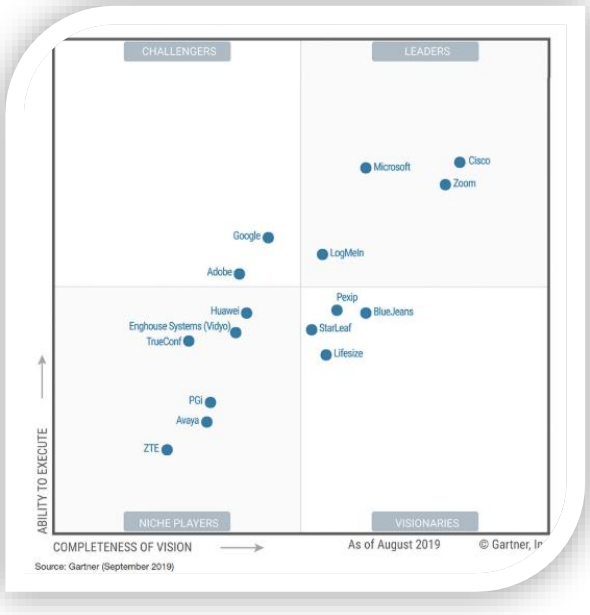


Ilustración 1: Cuadrante Mágico de Gartner 2019 para "Meeting Solutions"

4. Análisis de la plataforma Zoom para videoconferencias

Ahora que el mundo se encuentra en buena parte aislado a la par que intenta mantener sus actividades productivas, Zoom se ha convertido en una de las plataformas predilectas para realizar videoconferencias en esta cuarentena.

Durante las últimas semanas, la crisis de COVID-19 ha significado que millones de personas se queden en casa en lugar de ir a trabajar o reunirse con la gente. Las estimaciones varían, pero hasta el 60% de empleados a nivel global están trabajando desde sus hogares. Las plataformas de comunicación en línea se han vuelto esenciales para las interacciones personales y comerciales con el resto del mundo, y con una cuota de mercado mundial del 20%, Zoom es una de las plataformas más populares, ello dado por:

- Su simplicidad de uso para quien la administra
- Su simplicidad de uso para quien recibe la invitación y se conecta
- Rapidez para organizar teleconferencias.
- Permite grabar reuniones
- No te exige cuentas de sistemas para loguearte.
- Posibilidad de ver a todos los usuarios activos en la pantalla.

A. Ambigüedad en el tratamiento de los datos personales:

Es efectivo que se han publicado muchas vulnerabilidades sobre esta herramienta, pero según el historial de nuevas versiones, estas fallas se han solucionado. Las principales vulnerabilidades mencionadas son:

- Ambigüedad en el tratamiento de los datos personales
- Activación sin autorización de micrófono.
- Activación sin autorización de cámara web.

B. Últimas vulnerabilidades reportadas:

Desde la comunidad de investigadores se han reportado diversas vulnerabilidades para el aplicativo, que representan diversos grados de criticidad. En general se espera que la comunidad de investigadores siga protocolos de divulgación responsable de vulnerabilidades tales como ISO29147, pues estos protocolos dan tiempo suficiente a las empresas para resolver los problemas detectados y dan espacio también para el reconocimiento de los investigadores, no exponiendo tales debilidades abiertamente no estando aún la solución disponible.

Una de las últimas vulnerabilidades relevantes para el aplicativo zoom, habla de la posibilidad de que terceras partes pueden robar las credenciales de “login” (o acceso a su computador)

y ejecutar de manera arbitraria comandos en su sistema. Esta vulnerabilidad se clasifica como del tipo “UNC path injection”.

En la siguiente imagen se ilustra una posible explotación de la vulnerabilidad:

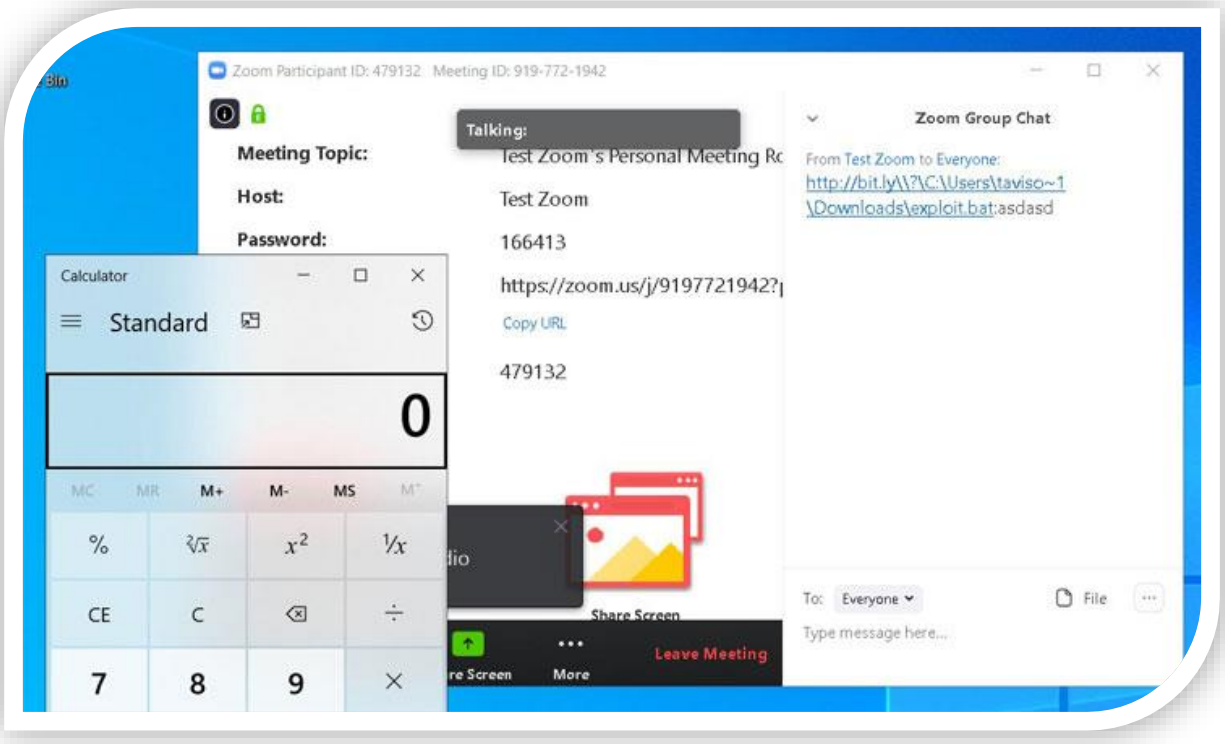


Ilustración 2: Posible ejecución de una vulnerabilidad en ZOOM (fuente imagen[7])

Es importante destacar que la empresa ha reconocido los problemas[8] y está reaccionando responsablemente dando solución a los problemas detectados y liberando versiones actualizadas del aplicativo que contienen código reparado y que soluciona los problemas informados.

Es importante considerar que, en esta relación de proveedor de aplicaciones y usuarios, ambos tienen que estar atentos a los problemas de ciberseguridad, pues el proveedor los debe detectar y solucionar, y los usuarios deben actualizar los aplicativos.

[7] https://thehackernews.com/2020/04/zoom-windows-password.html

[8] https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/

Para este caso en particular la empresa proveedora de ZOOM ha liberado[9] el 2 de abril la versión de zoom 4.6.9 (19253.0401), en la que:

- Se resolvió un problema por el cual una parte malintencionada podía usar enlaces UNC para filtrar la contraseña cifrada de un usuario.
- Se resolvió un problema por el cual algunos usuarios podían acceder al chat en un seminario web cuando el chat estaba deshabilitado.

Por este motivo CSIRT entrega la siguiente información y las recomendaciones para utilizar esta aplicación de forma segura durante el trabajo a distancia, las que aplican también para cualquier otra herramienta tecnológica de teleconferencia que usted como servicio desee utilizar.

C. Recomendaciones respecto a los usuarios de los sistemas:

1. Actualizar el software: para mantener los más altos niveles de seguridad, es clave contar con la última versión disponible de la aplicación, así como realizar actualizaciones de forma habitual. Al hacerlo, no sólo se añaden nuevas opciones y funcionalidades, sino que también se instalan parches de seguridad frente a fallos de seguridad detectados. La oportunidad para que los cibercriminales ataquen no se limita al momento en el que se produce la vulnerabilidad, sino que permanece activa hasta que los usuarios ejecuten la actualización del software y reciban los parches de los productos de la empresa para hacer frente a las amenazas. Esto significa que los usuarios que no han actualizado el software siguen siendo vulnerables. Zoom ya anunció la publicación de una versión para el día 6 de abril del 2020.

2. Utilizar un nombre de usuario y una contraseña: Las vulnerabilidades reportadas mostraban cómo un atacante podía adivinar números aleatorios asignados a las URL de una conferencia y penetrar en ellas sin alertar a los anfitriones. La brecha se produjo en conversaciones en las que no se establecieron contraseñas, lo que una vez más demuestra la importancia de utilizar este tipo de claves como primer nivel de seguridad. Tras resolver este fallo, Zoom adoptó nuevas medidas, utilizando passwords de forma automática en todas las reuniones programadas. La combinación de contraseña y mostrar el número de llamada es sinónimo de protección.

3. Utilizar formas seguras de invitar a los participantes: esta aplicación ofrece distintas formas de invitar a nuevos asistentes, como copiar la URL de la llamada y compartirla con cualquier contacto. Sin embargo, esta opción no requiere de contraseña para entrar, por

[9] https://support.zoom.us/hc/en-us/articles/201361953-New-Updates-for-Windows

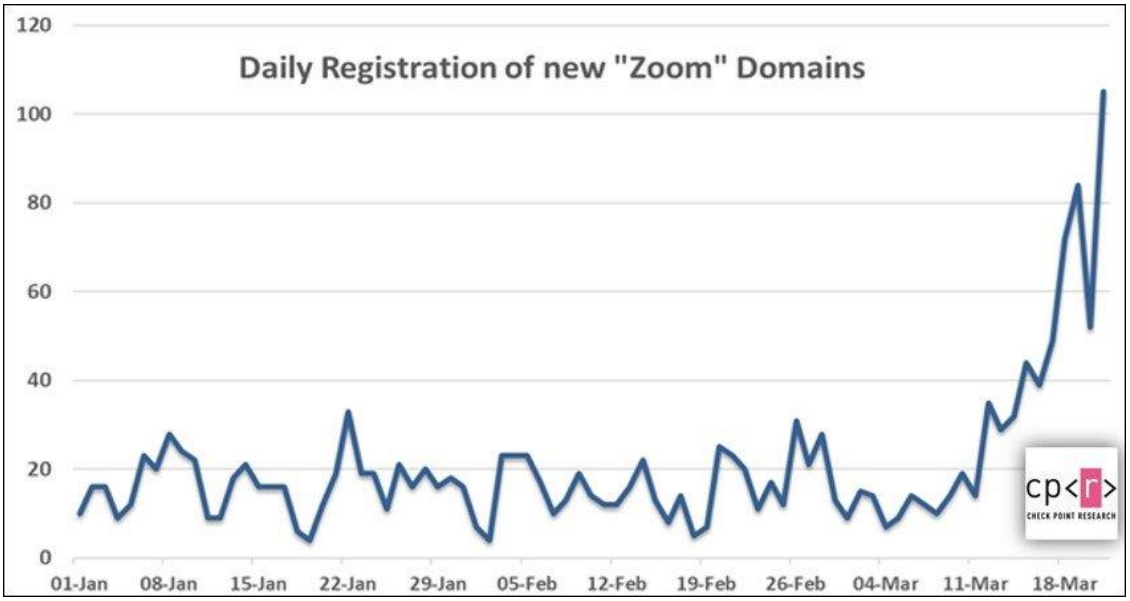
lo que ofrece pocas garantías. Por este motivo, se recomienda utilizar siempre el método seguro, que incluye el envío del identificador de llamadas y la contraseña de la llamada, así como conectarse a Zoom a través de SSO (Single Sign On) para un mayor nivel de seguridad.

4. Gestionar el acceso de los participantes: Incluso si hemos decidido utilizar la opción de compartir enlaces menos seguros, podemos evitar que los participantes muestren contenidos inapropiados restringiendo el uso de la cámara por parte de los participantes. El administrador de la conversación puede decidir quién puede usar su cámara y su micrófono haciendo clic en «Administrar participantes». Asimismo, otra forma de controlar quién entra en la llamada es la opción "Waiting room" en la que un gestor de llamadas crea una 'sala de espera' a través de la cual los participantes pueden conectarse, pero sólo si el gestor de llamadas confirma a los participantes uno por uno o en grupo. Esto se puede hacer en el menú desplegable «advanced options» cuando se desea programar una llamada.

5. Asumir que Zoom no ofrece privacidad absoluta: esta aplicación permite grabar llamadas de vídeo y exportarlas cuando termina la llamada. Es una herramienta muy útil cuando se quiere compartir información con otras personas que no pudieron asistir a la reunión. Sin embargo, esto también supone un problema, ya que cualquiera puede exportar la grabación, el archivo puede llegar a las manos equivocadas. Para reducir riesgos, el administrador de llamadas puede decidir qué participantes pueden grabar la llamada a través de la opción «Allow Record». Esto sólo protege frente al uso indebido de la aplicación, pero se puede utilizar algún software externo para grabar la conversación, por lo que no es posible garantizar al 100% la privacidad

6. Tener actualizado el Computador y Antivirus: es necesario para este tipo de modalidades de trabajo, contar más que nunca con los computadores de oficinas y de los hogares actualizados con las versiones más recientes del Sistema Operativo que utiliza (Windows, Linux, Mac) como contar también con un antivirus y actualizado para asegurarse que si existiesen nuevas fallas en los software de teleconferencia, estás puedan también ser bloqueadas por el computador o por el antivirus.

7. Tener cuidado de quien envía la invitación: Hay un aumento considerable de inscripción de dominios de internet asociados a la herramienta "Zoom" como a las otras más populares vigentes, se estima que muchos de esos dominios son para realizar estafas, suplantación de identidad y usurpación de datos personales o sensibles a través de envíos de phishing de posibles falsas reuniones por teleconferencia. Tal como lo muestra el siguiente cuadro obtenido por la empresa "Checkpoint".



Es fundamental revisar hoy más que nunca quien envía las invitaciones y no caer en estos intentos de phishing.

8. En caso de dudas contar siempre con soporte informático: Frente a los innumerables emails que puedan recibir, actualizaciones de software o uso de este tipo de herramientas, cuente siempre con el apoyo de las unidades de soporte informático de cada organización para subsanar dudas o capacitarse en el uso de estas herramientas.

9. Otras recomendaciones para un evento seguro que permiten las opciones avanzadas son:

   - No entregar el control de la pantalla compartida. Restringir que los participantes tomen control de la pantalla en un evento evitará que se comparta contenidos no deseado con el resto de los participantes.
   - Utilizar la versión pagada para garantizar soporte y responsabilidad de la empresa.
   - No grabar las reuniones, se pierde la encriptación de la comunicación de extremo a extremo.
   - Permitir solo participantes registrados. La inscripción de los participantes permite tener un control de los asistentes.
   - Colocar un doble factor de autenticación para el evento.
   - Remover a personas del evento si causan algún tipo de incidente.
   - Deshabilitar la opción de “unirse antes del anfitrión” para no perder el control de los asistentes de la reunión
   - Impedir la opción “permitir que los participantes eliminados se vuelvan a unir” para que la gente que ha sido expulsada del chat no pueda volver a ingresar

- Impedir la transmisión de archivos en el evento.
- Cerrar el evento una vez que se ha iniciado, para que no ingresen nuevos participantes, incluso si la persona tiene un ID de participación.
- No hacer reuniones públicas a través de la herramienta, sino sólo reuniones privadas, evitando con esto el "zoombombing".

IV.- Conclusiones:

CSIRT recomienda el uso de sistemas de teleconferencias a través de soluciones que transmitan en redes propias o del tipo "stand alone", como videoconferencia con hardware Polycom, Cisco, Microsoft, por sobre teleconferencia en la nube. De no ser posible esto, se recomienda el uso de los siguientes softwares o aplicativos que funcionan en Internet, que hasta la fecha hemos tenido la posibilidad de probar y utilizar, todo ello sin perjuicio que en el futuro nuevas herramientas puedan ser sumadas a este listado referencial que se adecuen a los estándares de ciberseguridad, tales como: "BlueJeans", "Cisco Webex", "Google Hangout Meet", "Microsoft Team", "Microsoft Skype", "Pexip" y "Zoom Meetings".

CSIRT no prohíbe el uso de ninguno de los softwares anteriormente mencionados.

CSIRT en cumplimiento del principio de neutralidad tecnológica de nuestra legislación deja a criterio de cada institución o servicio, la decisión técnica de que software o herramienta utilizará de las anteriormente señaladas, tomado en base la necesidad de cantidad de usuarios que requiera conectar, frecuencia de uso, la privacidad de la información que se compartirá en la reuniones como a sí mismo la criticidad de los servicios involucrados en las reuniones, que fue el caso de la decisión tomada por el Ministerio de Defensa para su comunicación interna.

CSIRT reconoce que todas las herramientas han tenido, tienen y tendrán vulnerabilidades, lo que podría afectar su seguridad informática, lo importante es que se actualicen por parte de la marca de una manera rápida y efectiva. Hacemos llamado a la comunidad a seguir las alertas de seguridad cibernéticas publicadas por el CSIRT y sobre todo considerar las recomendaciones de seguridad que este informe entrega. No existe una herramienta tecnológica perfecta por defecto, todas ellas implican recomendaciones de seguridad que deben ser aplicadas para que aseguremos nuestros servicios.

En caso de cualquier duda, no dude en contactar al CSIRT en modo 7x24 a través de los siguientes canales de comunicación:

En caso de requerir apoyo en implementación de sistemas de teleconferencia o de cambiar el actual que utilizan, sólo deben contactarnos en los números anteriormente mencionados.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.04.05 17:28:10 -04'00'