CÓMO GARANTIZAR LA SEGURIDAD EN LOS EVENTOS DIGITALES

La proliferación de eventos digitales e híbridos conlleva un mayor riesgo de ciberataques que pueden tener consecuencias devastadoras, tanto para los asistentes, cuyos datos personales quedan expuestos, como para la reputación de los organizadores.

Por **Cristina Cunchillos**

Con la llegada de la pandemia se aceleró el proceso de digitalización que estaba ya transformando hasta las actividades más mundanas: las compras *online*, la comunicación por videollamada, el ocio vía *streaming*... También el sector MICE recurrió al ámbito digital para su supervivencia, con reuniones, eventos, conferencias y ferias *online* cada vez más sofisticados.

Como consecuencia, el cibercrimen aumentó en un 600%, según la consultora de ciberseguridad Purplesec. Se estima que cada 39 segundos se produce algún tipo de ciberataque. El 2020 ya había sido un año récord en delitos de filtración de datos, en octubre de este año ese volumen ya se había superado en un 17%, según Fortune. Son estadísticas muy preocupantes.

Se estima que cada 39 segundos se produce algún tipo de ciberataque

El atractivo de los eventos digitales o híbridos para los cibercriminales es evidente. Además del contenido relacionado con la sesión, en una única plataforma *online* se gestionan los datos personales de miles de profesionales registrados, incluyendo directivos de grandes corporaciones de todo el mundo. Los organizadores, ahora más que nunca, tienen el deber de proteger esos datos y garantizar en la medida posible la seguridad del evento.

Las consecuencias de no hacerlo son nefastas. Un ciberataque puede resultar en pérdidas millonarias para las empresas hackeadas. Pero, más allá del impacto económico inmediato, puede dañar irreparablemente la reputación del organizador, y dar al traste con cualquier perspectiva de negocios futuros.

¿Videollamadas inofensivas?

Aunque un ciberataque en un evento digital de alto perfil tendrá más notoriedad, cualquier encuentro *online* supone un riesgo, incluso las simples videollamadas a través de plataformas como Zoom o Microsoft Teams con el resto del equipo cuando se trabaja remotamente. Se ha convertido en la vía habitual a la hora de mantener reuniones, internas o externas, y se prevé que continúe siéndolo mientras se reactiva el trabajo presencial en la oficina y los viajes de negocios, al menos para reuniones no esenciales.

La familiaridad ha hecho que a veces se descuide la seguridad. Por ejemplo, a veces se comparten a través de estas plataformas documentos con información confidencial o sensible. Por ello es esencial asegurarse de que solo personas autorizadas están presentes en la videoconferencia. También conviene que todos los participantes tengan una conexión a Internet segura, algo que no siempre se puede garantizar cuando se conectan desde casa o una red de *Wi-Fi* pública, como en un café o en la terminal de un aeropuerto.

Las plataformas de videoconferencias son un medio vulnerable. Más de medio millón de cuentas de Zoom han sido ya infiltradas y los datos de los usuarios vendidos a través de la Dark Web.

Tipos de ataques

Uno de los nuevos delitos que han surgido a raíz de la proliferación de eventos digitales es el llamado *zoom-bombing*. Es una forma de irrumpir en las reuniones virtuales por parte de personas que no fueron invitadas. Muchos buscan simplemente interrumpir con sus propios contenidos de propaganda, a veces abusivos, pero también pueden acceder a los datos de los participantes o la información que se esté compartiendo.

El 94% de los ciberataques se suelen realizar vía *e-mail*. En la mayoría de los casos se trata de fraude por *phishing*, o suplantación de identidad de una organización legal, engañando al usuario para que comparta información confidencial como datos bancarios. Se estima que en 2020 se crearon casi siete millones de páginas fraudulentas de *phishing*.

Para los eventos digitales, el mayor riesgo radica en los ataques de *ransomware*, o *malware* de rescate. Un *software* malicioso "secuestra" archivos, o incluso todo el equipo o dispositivo, de modo que nada es accesible a menos que se pague un rescate para liberar o descifrar esos datos, que han sido encriptados. Estos ataques bloquean absolutamente todo, haciendo imposible seguir adelante con cualquier actividad *online* que se estuviese llevando a cabo.

¿Qué se puede hacer?

Aunque no siempre es posible evitar un ciberataque, los organizadores de cualquier evento digital o híbrido, sea una simple videoconferencia o una feria virtual, pueden adoptar medidas preventivas para reducir los riesgos y estar mejor preparados para reaccionar.

• Lo primero es tener claro qué es exactamente lo que hay que proteger, qué datos se van a manejar y dónde van a estar. Y en todo momento. Hay que hacer un buen análisis de riesgos para establecer todas las posibles eventualidades. Solo así se podrá estar preparado.

• En el mundo virtual, "menos es más". Cuantos menos datos se manejen *online*, menos se pueden perder y, aunque puede ser tentador usar diferentes plataformas digitales –sobre todo para eventos híbridos–, es preferible integrarlas en un único sistema y protegerlo con una contraseña única.

• Del mismo modo, cuantas menos personas en la organización tengan acceso a los datos, menor será el riesgo. En todos los casos es importante que las personas involucradas en el evento virtual o híbrido, desde directivos al personal de recepción en la sede presencial, reciban la necesaria formación sobre los riesgos y los protocolos de seguridad que deben seguir.

• Hay que elegir bien la plataforma digital en la que se realizará el encuentro virtual, de acuerdo con las necesidades del cliente y asegurándose de que dispone de un sistema de seguridad sólido, además de ajustarse a las reglas del *compliance* y la normativa de datos vigente. También se debe exigir al proveedor que realice las comprobaciones pertinentes en todos los sistemas antes del evento.

• En videoconferencias, conviene solicitar que los participantes se identifiquen, incluso visualmente, y establecer el uso de contraseñas de acceso, o una sala de espera donde se controle a quien intente entrar. También se puede silenciar a los asistentes, desactivar los *chats* privados y limitar el uso compartido de pantallas. Siempre es mejor no compartir información sensible en la pantalla, que cualquiera puede guardar con una simple captura.

También los asistentes a eventos virtuales pueden contribuir a mejorar la ciberseguridad, asegurándose de que cuentan con un cortafuegos y un antivirus eficaz en sus instalaciones personales, manteniendo una buena "higiene de *e-mails*" y evitando el uso de redes de *Wi-Fi* públicas, menos seguras. Invertir en un *hotspot* móvil es una solución recomendable cuando se han de realizar desplazamientos profesionales frecuentemente.

> El 95% de los ciberataques son consecuencia de errores humanos

El 95% de los ciberataques son consecuencia de errores humanos, y no necesariamente de los miembros del equipo técnico encargado de la sesión.

Informar de su frecuencia y del modo de atajarlos a todos los actores implicados en un evento, incluyendo los asistentes, es ineludible para evitar pérdidas, a veces irrecuperables.

Bénédicte Losseau

Socia para Eventos y Operaciones en Exempla Management & Consulting

"Ya no se trata de prevenir si habrá un ataque, sino cuándo"

¿Por qué es importante cuidar de la ciberseguridad en reuniones, eventos y conferencias virtuales? ¿Se le ha dado la debida importancia durante la proliferación de encuentros *online*?

En mi opinión debería ser una prioridad a tomar muy en serio, ya que lo que está en juego son los atributos de la empresa, sus datos y su reputación. Se ha de pensar en lo que podría pasar y estimar el impacto que tendría el robo de datos, algo que siempre tendrá un impacto financiero negativo. Se daña la reputación del organizador y la confianza de los clientes, por lo que será más difícil atraerles en el futuro. La ciberseguridad es clave para la supervivencia de cualquier empresa, ya que no se trata de prevenir si habrá un ataque, sino cuándo, por eso tiene que estar preparada para mitigar los daños. Algunas estaban ya bien preparadas antes de la pandemia, pero otras están aún aprendiendo.

¿Cuál cree que es el error más común a la hora de proteger los datos e información en un evento virtual?

El mayor problema es cuando se ignora el factor humano. Se puede probar que la tecnología implementada funciona, pero si no se instruye bien al equipo que va a gestionar los datos sobre cómo hacerlo de forma segura y todas las posibles amenazas, como el *phishing* por ejemplo, se corre un gran riesgo. ¡Es tan fácil clicar en un enlace...! Muchos ataques no son el resultado de una planificación sofisticada sino de clicar en el enlace indebido. También es importante disponer de un plan de respuesta a crisis y saber qué hacer y cómo reaccionar rápidamente. Una respuesta rápida es esencial.

¿Cuál sería su principal recomendación a los organizadores de eventos virtuales e híbridos para protegerse de ciberataques?

En eventos híbridos y virtuales colaboran la tecnología y los humanos, por lo que hay que cuidar ambos aspectos. Por un lado, es imperativo instruir bien a la plantilla para que actúen como un cortafuegos y protejan los datos. Han de pensar siempre en términos de seguridad, y se tiene que gestionar bien el acceso que tienen a los datos de acuerdo con su posición. En cuanto a la tecnología, conviene hablar con los proveedores sobre los procesos de seguridad de la plataforma que se va a utilizar, planteando diferentes escenarios para identificar posibles debilidades y estar bien preparados ante cualquier imprevisto.