Confidencialidad en riesgo: evita filtraciones de información durante el teletrabajo

Inmersos en el teletrabajo, las videollamadas han resuelto la necesidad de comunicarse con clientes, proveedores y colaboradores, pero es difícil asegurar nuestra información mientras viaja por estos canales.

Alestra, empresa proveedora de **soluciones de innovación digital**, comparte datos de comportamiento interesantes: 90% de las personas que usan videoconferencias consideran que se expresan mejor; 25% de los colaboradores utilizan las videoconferencias para tener juntas más productivas, mientras que 35% considera que participar en videollamadas los hace sentir más valorados e incluidos en la compañía.

Existen riesgos que pueden comprometer áreas vitales de cualquier organización como los **ataques de phishing**, que aprovechan la debilidad emocional de las personas para obtener información clave desde datos financieros hasta información más sensible.

Las **amenazas a la ciberseguridad** son una realidad de la que México no está exento; su alarmante ritmo de crecimiento y sofisticación exige ocuparnos de ella de manera prioritaria, por lo que es imperativo replantearse la seguridad de forma integral para estar preparados, prevenir, detectar y responder de forma puntual a cualquier intimidación online que derive en un ataque cibernético y se materialice en la sustracción de activos o información confidencial de las organizaciones.

La ciberseguridad es labor de equipo y los colaboradores deben ser cautelosos en las herramientas de videoconferencia y envío de datos que utilizan. Entre los consejos que Alestra ofrece para **evitar caer en un ciberataque** son: tener reuniones en modo privado, solicitar una contraseña, iniciar hasta que el anfitrión de la reunión esté presente, permitir solo a usuarios previamente registrados, evitar grabar las sesiones, bloquear la reunión, controlar quién puede compartir pantalla, desactivar las funciones de guardar conversaciones o chats privados, entre otros.

No podemos hablar de qué plataforma o herramienta de videollamada es más conveniente; simplemente los corporativos deben ser más estrictos en el apego a sus lineamientos de software y licenciamiento y advertir a sus colaboradores con anticipación sobre lo que sí está permitido y los pasos a seguir para evitar ser víctima de un fraude cibernético.

En México, **el 77% de las organizaciones no cuenta con un sistema de respuesta contra incidentes.** Las consecuencias de ser víctimas de un ciberataque pueden afectar a las operaciones y traer implicaciones legales dependiendo de la información comprometida. Bajo esta perspectiva, las empresas expertas en sistemas integrados y automatizados ofrecen amplias coberturas ante posibles ataques, desde dispositivos de internet de las cosas, conectividad segura, nube y aplicaciones útiles para cualquier organización sin importar su tamaño o rubro.

La transformación digital mejora drásticamente la forma en que trabajamos y hacemos negocios; sin embargo, también introduce nuevos riesgos y más vale estar preparados para cualquier escenario con estrategias bien definidas y el soporte de una sólida área de TI dispuesta a detectar y responder de forma automática cualquier ciberamenaza.