Publicado en Mexico el 22/07/2022

# [DigiCert: Las empresas mexicanas deben tener una protección multifactor para evitar ataques de Ransomware](http://www.notasdeprensa.es)

## El ransomware sigue siendo una de las amenazas más preocupantes para las empresas, es por ello que es importante implementar soluciones sencillas pero altamente eficaces como la autenticación multifactor.

 El pasado mes de abril el grupo de ransomware conocido como "Conti" dirigió a organismos e instituciones de Costa Rica, su ciberataque masivo en forma de ransomware. Como es bien sabido, un ransomware es un software malicioso que secuestra la información de un sistema (como datos, archivos o claves) para pedir un rescate. El grupo atacó a 30 instituciones costarricenses como el Ministerio de Trabajo, el de Ciencia, Tecnología y Telecomunicaciones, el Seguro Social o el Instituto Meteorológico Nacional. Para el caso de México en el año 2019, un hacker logró infiltrarse en los equipos de la petrolera PEMEX  y posteriormente capturó una cantidad de documentos e información considerable por la que exigía alrededor de $96.8 millones de pesos mexicanos por su rescate. El pago, según el atacante, debía realizarse en 48 horas, de lo contrario publicaría toda la información en la Deep Web. Cómo consecuencia, los empresarios no podían realizar pedidos, las terminales de almacenamiento y distribución estaban congeladas y los trabajadores no tenían posibilidad de acceder al sistema informático de logística.  Según declaraciones oficiales de Pemex, el ataque fue llevado a cabo con un virus ransomware que afectó al menos al 5% de los equipos personales de cómputo. Ante estos relevantes casos de ataques cibernéticos en países de Latinoamérica, hoy es más que nunca es fundamental que las instituciones mexicanas tanto públicas como privadas, estén prevenidas, para  así evitar el robo de información y lograr que los ciberdelincuentes no ingresen a los escritorios remotos y al sistema de la empresa. Ante este panorama DigiCert recomienda el uso de autenticación multifactor, para crear una defensa de capas cuando la empresa aplica dos o más credenciales de acceso. La autenticación de múltiples factores se está volviendo más común con una tasa de crecimiento anual compuesta del 15% hasta 2025 particularmente en la industria financiera, y está avanzando para incluir escaneo de retina y huellas dactilares, reconocimiento de voz e incluso reconocimiento facial. Para mejorar la seguridad, la autenticación multifactor se puede incluir una contraseña, un token de seguridad y verificación biométrica. "Exigir múltiples factores para autenticar a un usuario hace que sea más difícil para una persona no autorizada obtener acceso a computadoras, dispositivos móviles, ubicaciones físicas, redes o bases de datos; cada capa sucesiva debería ayudar a proteger donde otras capas pueden ser débiles", afirma Dean Coclin, Director Senior de desarrollo comercial de DigiCert. "La protección de múltiples factores es fácil de implementar y fortalecerá inmediatamente la seguridad de una organización. Sin embargo, es importante considerar la seguridad en términos holísticos. Otros elementos, como la capacitación del personal y las herramientas que resuelven la suplantación de correo electrónico, complementan la protección multifactorial", agregó Roger Werner, director ejecutivo de CertSuperior. De hecho, la autenticación multifactor bloquea el 99,9% de los ataques automatizados, según Microsoft. En realidad, las contraseñas se pueden ver, escuchar, adivinar o omitir; una ficha se puede perder o robar; y un gemelo idéntico o el uso de una fotografía pueden incluso funcionar para engañar a los sistemas de reconocimiento biológico. El valor de la seguridad mediante la autenticación multifactor, si bien puede haber una debilidad en un factor de autenticación, por ejemplo, una contraseña o PIN robado, la fortaleza de un segundo o tercer factor compensa a los demás y fortalece el acceso a un sistema o plataforma. El número de empresas que utilizan la autenticación multifactor sigue en aumentoLas firmas financieras y otras empresas orientadas al consumidor prefieren la autenticación multifactor. Según el estudio de LastPass realizado en 2019, el 57% de las empresas encuestadas utilizan actualmente la autenticación multifactor, y se prevé que para finales de este año, el 90% de las empresas utilizarán este tipo de solución. El estudio asegura que, en ciberseguridad, hacer bien lo básico a menudo tiene el mayor impacto en la prevención de los ataques más comunes, por lo que se espera ver un uso más generalizado de la autenticación multifactor en todos los sectores en los próximos años. La forma de implementar la autenticación multifactorLas empresas necesitan coordinar y configurar la infraestructura para que los inicios de sesión protegidos funcionen correctamente durante el uso y soporte de herramientas multifactoriales. Las herramientas utilizadas para la autenticación multifactor incluyen varios agentes de software que pueden proteger VPN, servidores de SharePoint, Outlook Web App y servidores de bases de datos. DigiCert y Certsuperior recomiendan a las empresas mexicanas evaluar cuidadosamente los productos de autenticación de múltiples factores, para determinar cómo cada uno difiere sutilmente con respecto a la implementación deseada. Algunas preguntas que las empresas deben hacer durante sus soluciones de autenticación multifactor son: ● ¿Cuánta información privada maneja la red? ● ¿Quién necesitará ver los informes producidos por estos productos? ● ¿La empresa requiere la capacidad de ampliar la implementación? ● ¿Quiénes estarán entre la colección inicial de usuarios piloto? ● ¿Los empleados ya utilizan las herramientas de autenticación de dos factores disponibles con algunos servicios al consumidor? ● ¿Cómo se manejará un restablecimiento de contraseña en un entorno de autenticación de múltiples factores? La autenticación multifactor requiere una planificación avanzada y las empresas deben considerar muchos aspectos de la infraestructura de TI. Además, si la organización tiene un personal distribuido geográficamente, con pocas personas en muchas ciudades, puede ser difícil capacitar a la población de usuarios o difundir llaveros físicos; en estos casos, las empresas pueden querer buscar tokens de software o aplicaciones de software.

**Datos de contacto:**

PR DigiCert Latam

3125893314

Nota de prensa publicada en: [https://www.mexicopress.com.mx/la-importancia-de-una-proteccion-multifactor](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: Software Ciberseguridad Dispositivos móviles



[**http://www.mexicopress.com.mx**](http://www.notasdeprensa.es)